Citrix Gateway service

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Release Notes 2

Get started with Citrix Gateway service 22

Technical security overview 22

Geo-location Routing 26

Migrate NetScaler Gateway to Citrix Gateway service for HDX Proxy 28

HDX Adaptive transport with EDT support for Citrix Gateway service 33

Network metrics monitoring for Citrix Gateway service 37

Citrix Gateway service on Google Cloud Platform 40

Support for Citrix Virtual Apps and Desktops 42

Citrix Gateway Service for StoreFront 43

Support for the Citrix DaaS environments 49

Support for on-premises Citrix Virtual Apps and Desktops 51

List of Points of Presence (PoPs) for Citrix Gateway service 54

PoPs for commercial regions 55

PoPs for Google Cloud Platform (GCP) customers 60

PoPs for Japan region 62

PoPs for US Government region 64

Cloud Connector sizing and scale considerations for HDX proxy 65

FAQ 67

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release Notes

October 15, 2026

The Citrix Gateway service release to cloud release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes include one or more of the following sections:

What's new: New features and enhancements available in the current release.

Fixed issues: Issues that are fixed in the current release.

Known issues: Issues that exist in the current release and their workarounds, wherever applicable.

September 04, 2026

What's new

- **Deprecated ciphers**

  Citrix Gateway service will no longer support the following ciphers after September 2026.

  - TLS1.2-ECDHE-RSA-AES-256-SHA384
  - TLS1.2-AES256-GCM-SHA384
  - TLS1-AES-256-CBC-SHA

  [CTXENG-66589]

September 02, 2026

What's new

- **Enhanced Citrix Gateway service upgrades**

  Citrix Gateway service now uses a phased approach for service upgrades, providing a more controlled upgrade process that improves service reliability, reduces potential disruption, and dependency on maintenance windows.

  > **Important:**
  >
  > - Customers who already allowlist `*.nssvc.net`, the more specific `*.g.nssvc.net` and `*.c.nssvc.net` domains, or the published Citrix Gateway service FQDNs, do not need to take any action.
  > - If your environment restricts Citrix Gateway service connectivity by IP address, review

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> your current configuration against the published connectivity requirements. Citrix recommends using FQDN-based rules, because the destination IP addresses for the Citrix Gateway service can change.

For more information, see:
System and Connectivity Requirements.
List of PoPs.

[CTXENG-73445]

July 06, 2026

What's new

- **Citrix Gateway service PoP expansion**

  To enhance business continuity and ensure quality of service for customers using Citrix Gateway service for HDX proxy, the following new PoP has been launched on July 01, 2026.

PoP code	PoP FQDN	Cloud service provider	Country	Location
aws-asia-tw	aws-asia-tw-rdvz.g.nssvc.net	AWS	Taiwan	Taipei

June 25, 2026

What's new

- **Citrix Gateway service PoP expansion**

  To enhance business continuity and ensure quality of service for customers using Citrix Gateway service for HDX proxy, the following new PoPs have been launched on June 19, 2026.

PoP code	PoP FQDN	Cloud service provider	Country	Location
az-in-c	az-in-c-rdvz.g.nssvc.net	Azure	India	Pune
az-eu-c	az-eu-c-rdvz.g.nssvc.net	Azure	Germany	Frankfurt

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoP code	PoP FQDN	Cloud service provider	Country	Location
az-us-c	az-us-c-rdvz.g.nssvc.net	Azure	USA	Iowa
aws-eu-s	aws-eu-s-rdvz.g.nssvc.net	AWS	Italy	Milan

For more information, see PoP FQDNs.

[CTXENG-70027]

March 25, 2026

What's new

- **Support for geo-location routing for Global - Alternate region**

  Citrix Gateway service now supports geo-location routing for Global - Alternate region.

  The following table lists the Global - Alternate region FQDNs and PoPs for geo-location routing:

Geo-location	FQDNs	PoPs included
Global-Alternate	• global-alt-rgn.g.nssvc.net - global-alt-rgn-s.g.nssvc.net	az-asia-se, az-aus-e, az-bz-s, az-ca-c, az-eu-n, az-eu-w, az-in-s, az-jp-e, az-nw-e, az-uae-n, az-us-e, az-us-sc, az-us-w, az-za-n, aws-aus-e, aws-bz-s, aws-ca-e, aws-eu-c, aws-in-w, aws-uk-se, aws-us-e, aws-us-nc, aws-us-w, az-us-e2, aws-asia-se, aws-eu-w, aws-in-sc, aws-jp-w

[CTXENG-69235]

- **Support for geo-location routing for India region**

  Citrix Gateway service now supports geo-location routing for the India region.

  The following table lists the India region FQDNs and PoPs for geo-location routing:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Geo-location	FQDNs	PoPs included
India	• india-rgn.g.nssvc.net.akadns.net - india-rgn-s.g.nssvc.net.akadns.net	aws-in-w, aws-in-sc, az-in-s

[CTXENG-69234]

March 13, 2026

What's new

- **Citrix Gateway service PoP expansion**

  To enhance business continuity and ensure quality of service for customers using Citrix Gateway service for HDX proxy, launch of the following new PoPs is planned by the end of May 2026:

PoP code	PoP FQDN	Cloud service provider	Country	Location
az-in-c	az-in-c-rdvz.g.nssvc.net	Azure	India	Pune
az-eu-c	az-eu-c-rdvz.g.nssvc.net	Azure	Germany	Frankfurt
az-us-c	az-us-c-rdvz.g.nssvc.net	Azure	USA	Iowa
aws-eu-s	aws-eu-s-rdvz.g.nssvc.net	AWS	Italy	Milan

For more information, see PoP FQDNs.

[CTXENG-70027]

March 11, 2026

What's new

- **TLS 1.3 support for Citrix Gateway service**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway service will enable end-to-end TLS 1.3 connections by the middle of Q3, 2026. This upgrade is part of our ongoing commitment to improve security, performance, and compliance.

Customer actions

Customers leveraging Rendezvous with Citrix Gateway service must ensure that their Virtual Delivery Agent (VDA) deployments meet the minimum supported versions to prevent potential session launch issues.

- Minimum VDA version requirements for TLS 1.3:
  - Current Release (CR): 2407 or later
  - Long Term Service Release (LTSR): 2402 LTSR CU1 or later
- Citrix Workspace app (CWA) requirements:

  Citrix Workspace app version that explicitly supports TLS 1.3. Verify client operating system versions that support TLS 1.3 by reviewing the Citrix Workspace app feature matrix. For more information, see Citrix Workspace app feature matrix.

> **Note:**
>
> **Critical upgrade warning for specific VDA versions:**
>
> Upgrade older VDAs, such as CR 2303, CR 2308, CR 2311, or LTSR 2402 (prior to CU1) to the minimum supported versions before the middle of Q3, 2026. This prevents potential session launch failures and ensures uninterrupted service.
>
> **TLS 1.2 Fallback:**
>
> Older supported VDA versions that do not natively support TLS 1.3 such as 2203 LTSR CUs, CR VDAs before 2303 or connections made through older supported versions of the Citrix Workspace app that do not natively support TLS 1.3, continue to operate without session launch issues. These connections safely continue to work with TLS 1.2.
>
> For more information on VDA version support, see Upgrade and migrate. For more information on deployment planning, see Citrix LTSR and Current Release lifecycle documentation.

[CTXENG-67714]

October 16, 2025

What's new

- **Network metrics monitoring - General availability in Citrix Gateway service**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network metrics monitoring is now generally available in Citrix Gateway service. For more information, see Network metrics monitoring for Citrix Gateway service.

[CTXENG-65466]

October 08, 2025

What's new

- **Support for on-premises Citrix Virtual Apps and Desktops - General availability in Citrix Gateway service for StoreFront**

  Support for on-premises Citrix Virtual Apps and Desktops is now generally available in Citrix Gateway service for StoreFront. For more information, see Support for on-premises Citrix Virtual Apps and Desktops.

  [CTXENG-1466]

September 30, 2025

What's new

- **Cloud Connector sizing and scale recommendations for HDX proxy**

  Updated Cloud Connector sizing and scale recommendations are now available for HDX proxy deployments that do not use the Rendezvous v1 or v2 protocol. This guidance ensures high availability, stability, and efficient performance. For more information, see Cloud Connector sizing and scale considerations for HDX proxy.

  [CGS-21614]

September 24, 2025

What's new

- **Addition of AWS PoP in Osaka, Japan**

  To enhance business continuity and ensure quality of service for customers using the Citrix Gateway service for HDX proxy, we are adding a new PoP in Osaka, Japan.

  PoP FQDN: aws-jp-w-rdvz.g.nssvc.net

  For more information, see PoP FQDNs.

  [CTXENG-67498]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

August 19, 2025

What's new

- **DNS service changes in the Citrix Gateway service**

  The Citrix Gateway service is migrating its DNS service from the current provider to Akamai DNS for the Citrix commercial cloud in a phased manner. To ensure a smooth migration and continued operation, you must complete the following configurations:

  1. **Firewall configuration:** Configure firewalls and Secure Web Gateways as mentioned in System and Connectivity Requirements. Ensure all the global FQDNs are part of your required exceptions. For more information, see Global FQDNs with defined set of PoPs.
  2. **DNS forwarder configuration:** If DNS forwarders are configured to allow recursive DNS resolution for specific domains, you must include `*.akadns.net` in the allowed list. This configuration enables Citrix Cloud Connector, Citrix Virtual Apps and Desktops, or client to connect to the Citrix Gateway service.

  [CTXENG-67839]

August 07, 2025

What's new

- **Citrix Gateway service PoP expansion**

  To enhance business continuity and ensure quality of service for customers using Citrix Gateway service for HDX proxy, launch of the following new PoPs are planned for the upcoming service release:

PoP code	PoP FQDN	Cloud service provider	Country	Location
az-us-e2	az-us-e2-rdvz.g.nssvc.net	Azure	USA	Virginia
aws-asia-se	aws-asia-se-rdvz.g.nssvc.net	AWS	Singapore	Singapore
aws-asia-tw	aws-asia-tw-rdvz.g.nssvc.net	AWS	Taiwan	Taipei

  For more information, see PoP FQDNs.

  [CTXENG-67498]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Support for Citrix Gateway service bandwidth monitoring in Citrix Japan Cloud**

  Administrators of Citrix Japan Cloud can now monitor Citrix Gateway service bandwidth usage with enhanced visibility and tracking capabilities. This feature provides comprehensive insights into consumption patterns across multiple entitlements and enables proactive monitoring of bandwidth usage to identify potential overages.

  The following are some of the key features:

  - **Usage summary:** The **Usage Summary** page displays an overview of all your entitlements and any bandwidth overage.
  - **Detailed usage interface:** A multi-tab interface allows you to view usage details of your monthly, annual, and termed entitlements.
  - **Entitlement-based calculation:** Bandwidth is precisely calculated based on the allocation of your purchased entitlements.

  For more information, see Monitor bandwidth usage for Gateway service.

  [CTXENG-602]

June 19, 2025

What's new

- **Enhanced network metrics monitoring for the Citrix Gateway service - Preview**

  The enhanced network metrics monitoring for the Citrix Gateway Service is now available to all Citrix DaaS™ customers. To use this feature, admins must only enable the **Network telemetry** policy in Citrix Studio or Web Studio for the following builds:

Component	Platform	Supported version
Citrix Workspace app	Windows	2411 or later
Citrix Virtual Apps and Desktops	Windows	2411 or later

  [CTXENG-65466]

Known issues

- The session reliability feature might not work for EDT sessions when the **Network telemetry** policy is enabled for version 2503 of both Citrix Workspace app and Citrix Virtual Apps and Desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

[CGS-21605]

June 12, 2025

What's new

- **Support for on-premises Citrix Virtual Apps and Desktops - Preview**

  The Citrix Gateway service now supports on-premises Citrix Virtual Apps and Desktops. The Citrix Gateway service is integrated with the on-premises Delivery Controller, which makes hybrid access easier for Citrix Virtual Apps and Desktops customers. Hybrid access lets you use your on-premises NetScaler Gateway and StoreFront for authentication, authorization, and enumeration. Citrix Gateway service is used to launch virtual apps and desktops. This approach maximizes the value of existing remote access infrastructure and minimizes administrative effort.

  Key benefits:

  The integration of Citrix Gateway service with on-premises Delivery Controller offers the following benefits:

  - **Customization retention:** NetScaler Gateway and StoreFront™ customizations can be retained, ensuring a consistent user experience.
  - **Minimized maintenance:** HDX proxy performance and scale requirements are now managed by Citrix Gateway service, eliminating the need for customer management.
  - **Existing URL:** DaaS customers can continue using their familiar on-premises NetScaler® Gateway URL.
  - **Leveraging LHC for enhanced resiliency:** Local Host Cache (LHC) supports resiliency needs by allowing the connector to function as a local Secure Ticket Authority (STA) during outages.
  - **Better user experience:** Ability to use geographically closer PoPs reduces latency and improves performance.
  - **High resiliency:** Ensures high resiliency because of the multi-cloud and multi-geo architecture of Citrix Gateway service.

  Prerequisites:

  1. You must have a functional on-premises working environment where NetScaler Gateway is used for authentication and authorization and StoreFront is used for enumeration.
  2. Upgrade StoreFront to version 2503 or higher. For more information, see Upgrade StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a resource location on Citrix Cloud™:

1. Onboard to Citrix Cloud. For more information, see Create a Citrix Cloud account and Connect to Citrix Cloud.
2. On Citrix Cloud, install Cloud Connectors and associate them with the resource location. For more information, see Cloud Connector Installation.

   > **Note:**
   >
   > To make your existing apps and desktops available to subscribers, add your site (Citrix Virtual Apps and Desktops deployment) to Citrix Workspace. For more information, see Aggregate Virtual Apps and Desktops in workspaces.

Configure the resource location and policies on the on-premises Delivery Controller™:

1. Run the following command on the Windows Active Directory (AD) or Domain Controller (DC) server, to retrieve the Security Identifiers (SIDs) of connector machines in a Windows AD or DC environment. Note the SIDs of the connector machines.

   ```
   Get-ADComputer -Filter *|Select-Object Name, SID
   ```

2. In the on-premises Delivery Controller, create a zone and map it to the resource location created in Citrix Cloud.

   a) In on-premises Delivery Controller, run the following command in the PowerShell and note the Uid generated for the required resource location:

   ```
   Get-ConfigZone
   ```

   b) Run the following commands for all the Citrix Cloud Connectors:

   ```
   Set-ConfigZone -Uid <Uid from above command output> -
       ExternalUid <RL ID noted at step 1>

   new-configedgeserver  <User friendly name> -MachineAddress
       "<Connector FQDN"> -Sid <Connector respective SID from
       step 2> -uuid <Respective Edge server UUID from step 1>
       -ZoneUid <Uid from Get-ConfigZone output>
   ```

3. To use Rendezvous v1, enable Rendezvous within the Delivery Controller policies and ensure that the on-premises Delivery Controller is configured with the connector details to accept Rendezvous requests. For more information, see Rendezvous v1.
4. To use HDX adaptive transport with EDT, enable adaptive transport protocol within the Delivery Controller policies on your on-premises Delivery Controller. For more information, see HDX Adaptive transport with EDT support for Citrix Gateway service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Citrix Gateway service for StoreFront to integrate with on-premises Delivery Controller:

Perform the following steps to integrate the Citrix Gateway service for StoreFront with the on-premises Delivery Controller:

1. Configure an authentication gateway
2. Configure a routing gateway
3. Configure remote access setting for Delivery Controller
4. Map the Delivery Controller and routing gateway
5. Configure the optimal HDX™ gateway routing

Step 1 - Configure an authentication gateway:

1. Open the StoreFront management console.
2. Navigate to **Stores** > **Manage Citrix Gateways** and click **Add**.
3. In **Display name**, enter a name for the authentication gateway.
4. In **Gateway type**, select **Citrix Gateway Appliance** and in **Usage or role**, select **Authentication only**.
5. In **Citrix Gateway URL**, enter an authentication URL.
6. Click **Next** and then **Finish**.

Step 2 - Configure a routing gateway:

1. Navigate to **Stores** > **Manage Citrix Gateways** in the StoreFront management console and click **Add**.
2. In **Display name**, enter a name for the routing gateway.
3. In **Gateway type**, select **Citrix Gateway service**.
4. If geo-location routing is required, fill the following parameters:
   - **Citrix Gateway service URL:** Enter the FQDN ending with `rgn.g.nssvc.net`, which serves as the general FQDN for geo-location routing.
   - **Citrix Gateway service URL (STA Connector Mode):** Enter the FQDN ending with `rgn-s.g.nssvc.net`, which supports the service continuity feature.

   For more information, see Regional FQDNs for geo-location routing.
5. Navigate to the **Cloud Connectors** tab and click **Add** to add the cloud connector URLs.
6. Enable **Load balance multiple servers** and **Enable session reliability**.
7. Click **OK**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - HDX session launch fails if the **Enable session reliability** option is disabled on on-premises StoreFront.
> - Citrix Gateway service for StoreFront does not support dual STA. Hence, the **Request two tickets from cloud connectors, where available** option must not be selected.

Step 3 - Configure remote access setting for Delivery Controller:

1. In the StoreFront management console, navigate to **Configure remote access settings** in your site.
2. Select **Enable remote access**.
3. In **Citrix Gateway**, select the previously configured authentication gateway.
4. Click **OK**.

Step 4 - Map Delivery Controller and routing gateway:

1. In the StoreFront management console, navigate to **Configure store settings** > **Optimal HDX routing** in your site.
2. Select the routing gateway, click **Manage sites**, and select the configured site.
3. Click **OK**.

Step 5 - Configure optimal HDX gateway routing:

> **Note:**
>
> If you have multiple zones, create routing gateways for each zone as given in "Step 2: Configure a routing gateway".

Map each zone to its distinct routing gateway as given in the following steps:

1. In the StoreFront management console, navigate to **Configure store settings** > **Optimal HDX routing** in your site.
2. Select the routing gateway and click **Manage zones**.
3. Click **Add** under **Manage zones** and create a zone with the same zone name created at the on-premises Delivery Controller.

[CTXENG-1466]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

June 05, 2025

What's new

- **Addition of AWS PoP in Paris, France**

  To enhance business continuity and ensure quality of service for customers using Citrix Gateway service for HDX proxy, a new AWS PoP is added in Paris, France.

  PoP FQDN: aws-eu-w-rdvz.g.nssvc.net

  For more information, see PoP FQDNs.

  [CGS-21400]

May 20, 2025

What's new

- **Security and compliance enhancements**

  Citrix Gateway service is now compliant with the following industry-standard certifications, reinforcing our commitment to delivering a secure and reliable service:

  - **System and Organization Controls (SOC) 2 Type 2:** Ensures compliance with stringent requirements for security, availability, processing integrity, confidentiality, and privacy.
  - **Payment Card Industry Data Security Standard (PCI DSS) v4.0:** Validates the secure handling of payment card data.
  - **Health Insurance Portability and Accountability Act (HIPAA):** Demonstrates adherence to regulations for the secure management of protected health information (PHI).

  For the latest certification status, see the "Certifications"section in Citrix Trust Center.

  [CTXENG-65435]

May 15, 2025

What's new

- **Geo-location Routing - General availability in Citrix Gateway service for StoreFront**

  Geo-location Routing is now generally available in Citrix Gateway service for StoreFront. For more information, see Add Citrix Gateway service.

  [CGS-21536]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

May 13, 2025

What's new

- **Addition of AWS PoP in Hyderabad, India**

  To enhance business continuity and ensure quality of service for customers using Citrix Gateway service for HDX proxy, a new AWS PoP is added in Hyderabad, South-Central India.

  PoP FQDN: aws-in-sc-rdvz.g.nssvc.net

  For more information, see PoP FQDNs.

  [CTXENG-67122]

March 27, 2025

What's new

- **Support for geo-location routing to PoPs in Asia region**

  Citrix Gateway service now supports geo-location routing to PoPs in the Asia region.

  The following table lists the Asia region FQDNs and PoPs for geo-location routing:

Geo-location	FQDNs	PoPs included
Asia	• asia-rgn.g.nssvc.net • asia-rgn-s.g.nssvc.net	az-uae-n, aws-in-w, az-in-s, az-asia-se, az-jp-e

  [CTXENG-65014]

February 21, 2025

What's new

- **Enhanced Citrix DaaS experience for GCP customers with support to commercial region PoPs**

  The upcoming service release will provide support for PoPs in commercial regions for GCP customers.

  Currently, there are 24 commercial region PoPs across 5 continents. With this upcoming support, you can use these PoPs in Azure and AWS in addition to the existing GCP PoPs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> To ensure continued operations in your Citrix DaaS deployment, complete the instructions specified in PoPs for Google Cloud Platform (GCP) customers before March 15, 2025.

[CGS-20941]

January 20, 2025

What's new

- **Network metrics monitoring for Citrix Gateway service - Preview**

  The network metrics provide end-to-end visibility of HDX traffic between Citrix Workspace app and Virtual Delivery Agent (VDA) passing through Citrix Gateway service. The visual representation of network metrics in DaaS Monitor enables administrators to view real-time client and network latency metrics, historical reports, end-to-end performance data, and troubleshoot performance issues. For more information, see Network metrics monitoring in Citrix Gateway service - Preview.

  [CGS-17876, CGS-18276]

January 15, 2025

What's new

- **Geo-location Routing - General availability**

  Geo-location Routing is now generally available in Citrix Gateway service. For more information, see Geo-location Routing.

  [CGS-17232]

September 18, 2024

What's new

- **Citrix Gateway service for StoreFront - General availability**

  Citrix Gateway service for StoreFront is now generally available in the Citrix DaaS environments. See Citrix Gateway service for StoreFront

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Resiliency with Local Host Cache (LHC)**

  In a Citrix Gateway service for StoreFront deployment, LHC is activated when the communication between the Cloud Connector and Citrix Cloud is disrupted. LHC is a functionality of Citrix DaaS that ensures resiliency during network outages. For more information, see Resiliency with Local Host Cache (LHC).

  [BRK-15652]

April 25, 2024

What's new

- **Citrix Gateway service for StoreFront - Preview**

  Citrix Gateway service for StoreFront is a cloud-based HDX solution that provides secure remote access to resources accessed from on-premises StoreFront. You can leverage the scalability and reliability of Citrix Cloud (for HDX proxy) without changing your on-premises StoreFront and on-premises NetScaler Gateway environments.

  This solution is in preview. For details see Citrix Gateway service for StoreFront - Preview.

April 24, 2024

What's new

- **Support for loss tolerant mode for audio policy**

  Citrix Gateway service now supports the latest loss tolerant mode for audio in Citrix Virtual Apps and Desktops. This mode enhances the audio experience for users connecting to networks with high latency and packet loss. Users must use Citrix Virtual Apps and Desktops 7 2402 LTSR or later versions to use this functionality.

  The loss tolerant mode for audio is based on the EDT loss tolerant transport protocol, which allows packet loss in transmission without resending multimedia content, resulting in a more real-time experience for users. It is the preferred mode for audio during lossy network conditions to ensure superior audio quality compared to EDT.

  For details on the loss tolerant mode settings, see Loss tolerant mode for audio.

April 19, 2024

What's new

- **Support for Toronto (Canada) Azure PoP**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for the Azure PoP in Toronto, Canada is now available.

PoP FQDN: `az-ca-c-rdvz.g.nssvc.net`

For details, see Geo-location Routing - Preview.

[CGS-12933]

February 27, 2024

What's new

- **Support for Google Cloud Platform**

  Support for Google Cloud Platform (GCP) PoPs along with the existing Azure and AWS PoPs are planned in the upcoming service releases.

  Currently, there are 5 GCP PoPs that are distributed across geo-locations. With this upcoming support, you can leverage these GCP PoPs along with the existing Azure and AWS PoPs.

  > **Important:**
  >
  > To ensure continued operations in your Citrix DaaS deployment, complete the instructions specified in Citrix Gateway service –Points-of-Presence (PoPs) before 15th of March 2024.

February 01, 2024

What's new

- **Support for Toronto (Canada) Azure PoP**

  Support for the Azure PoP in Toronto, Canada is planned in the upcoming service releases.

  PoP FQDN: `az-ca-c-rdvz.g.nssvc.net`

  [CGS-12933]

November 02, 2023

What's new

- **Support for the latest version of reducer for HDX**

  Citrix Gateway service supports the latest version of the reducer for HDX. Reducer for HDX is a general purpose compressor that works across virtual channels. The latest reducer improves the overall performance of Citrix DaaS with the following capabilities:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Reduces the network bandwidth utilization for HDX sessions.
- Data packets are transmitted in a shorter duration, resulting in a faster response.

The following software versions support the latest reducer.

- Citrix Virtual Apps and Desktops 7 2303 (Windows) and later.
- Citrix Workspace app 2303 (Windows) and later.

[CGS-16258]

August 29, 2023

What's new

- **Geo-location Routing - Preview**

  Citrix Gateway service provides a capability to the admins to enable their users to connect to PoPs in a particular region or only through a particular cloud service provider regardless of the users' location. For more information, see Geo-location Routing - Technical preview.

  [CGS-13782]

- **HDX Performance Analytics**

  Citrix Gateway service supports the HDX performance analytics functionality that enables Citrix Analytics administrators to view performance data related to the Connector-Gateway PoP latency. For more information, see Connector Statistics.

  [CGS-15829]

- **Accelerated Networking**

  The Citrix Gateway service infrastructure is enhanced to support accelerated networking wherein it uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities to users.

  [CGS-15684]

- **Deprecated weak ciphers**

  For the updated list of the deprecated ciphers of Citrix Gateway service, see Technical security overview.

  [CGS-14234]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixed issues

- EDT sessions are disconnected whenever the backend pool is modified in the Azure load balancer.

  [CGS-15808]

November 10, 2022

What's new

- **Rendezvous protocol version V2 support**

  The Citrix Gateway service now supports Rendezvous protocol version V2 for Citrix Gateway service on the Google Cloud Platform. For details, see Citrix Gateway service features supported.

- **Citrix Gateway service on Google Cloud Platform availabiality in Europe**

  Citrix Gateway service on the Google Cloud Platform is now available in Europe in the following regions.

  - London
  - Zurich

  For details, see Citrix Gateway service on Google Cloud Platform.

Known issues

- Rendezvous v2 VDA registration fails if the customer ID is fewer than 6 characters.

  [CGS-15036]

June 30, 2022

What's new

- **Citrix Gateway service availability on the Google Cloud Platform**

  With Citrix Gateway service support on the Google Cloud Platform (GCP), customers running their workloads on Google Cloud can take the advantage of Google Cloud's high-performing global network using the Citrix Gateway optimal routing feature. The optimal gateway routing feature directs clients to the closest GCP Citrix Gateway service PoP. Also, the Citrix Gateway service on Google Cloud provides secure connectivity between Citrix Workspace clients and virtualization resources to deliver sessions with the lowest latency and the best user experience possible. For details, see Citrix Gateway service on Google Cloud Platform.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

April 04, 2022

What's new

- **Rebranding changes**
  - Citrix Secure Workspace Access is now rebranded to Citrix Secure Private Access.
  - Citrix Virtual Apps and Desktops service is now rebranded to Citrix DaaS.

What's new

- **Merger of Citrix Gateway service tile into a single Citrix Secure Private Access in Citrix Cloud**

October 11, 2021

What's new

- **Merger of Citrix Gateway service tile into a single Citrix Secure Private Access in Citrix Cloud**

  The Citrix Gateway service tile and Citrix Secure Private Access tile are merged into Citrix Secure Private Access tile and the Citrix Gateway landing page is modified for Citrix Secure Private Access. Therefore you do not see the **Virtual Apps and Desktops** and the **Add a Web/SaaS app** shortcuts. However, the Citrix Virtual Apps and Desktops customers can enable Citrix Gateway service from **Workspace configuration > Access > External Connectivity**. There is no change in the functionality, otherwise.

  The following Citrix Gateway service features are moved to Citrix Secure Private Access service.

  - Configuring SaaS and Enterprise web apps
  - Enabling enhanced security controls
  - Configuring contextual policies

  Citrix Secure Private Access customers, including Citrix Workspace Essentials and Citrix Workspace Standard, can now use one single Citrix Secure Private Access tile for configuring SaaS and Enterprise web apps, enhanced security controls, contextual policies, in addition to web filtering policies.

  [ACS-645]

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Get started with Citrix Gateway service

September 30, 2026

Customers who are entitled for the Citrix DaaS get the Citrix Gateway service enabled, by default. Customers do not have to request a separate Citrix Gateway service trial. For details, see Sign up for the service.

> **Important:**
>
> On the Citrix Cloud home page, you do not see the Citrix Gateway service tile. The Citrix Gateway service tile and Citrix Secure Private Access tile are merged into Citrix Secure Private Access tile and the landing page is modified for Citrix Secure Private Access. Therefore you do not see the **Virtual Apps and Desktops** shortcut. However, the Citrix Virtual Apps and Desktops customers can enable Citrix Gateway service from **Workspace configuration > Access > External Connectivity**. There is no change in the functionality, otherwise.

Technical security overview

October 15, 2026

Citrix Cloud manages the operation for Citrix Gateway services, replacing the need for customers to manage the NetScaler Gateway appliance. Citrix Gateway service is provisioned through Citrix Workspace app.

Citrix Gateway service provides the following capabilities:

HDX Connectivity: The Virtual Delivery Agents (VDAs) hosting the apps and desktops remain under the customer's control in the data center of their choice, either cloud or on-premises. These components are connected to the cloud service using an agent called the Citrix Cloud Connector.

DTLS 1.2 protocol support: Citrix Gateway service supports Datagram Transport Layer Security (DTLS) 1.2 for HDX sessions over EDT (UDP-based transport protocol). The following cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS protocol support: Citrix Gateway service supports the following TLS cipher suites:

- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES-256-SHA384

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-AES256-GCM-SHA384
- TLS1-AES-256-CBC-SHA

> **Note:**
>
> Citrix Gateway Service does not support TLS 1.0 and TLS 1.1 versions.

Endpoint Management integration: When integrated with Citrix Endpoint Management plus Citrix Workspace, the Citrix Gateway service provides secure remote device access to your internal network and resources. Onboarding the Citrix Gateway service with Endpoint Management is fast and simple. The Citrix Gateway service includes full support of Citrix SSO for apps such as Secure Mail and Secure Web.

Data flow

Citrix Gateway service is a globally distributed multitenant service. End users use the nearest Point-of-Presence (PoP) where the particular function that they need is available, regardless of Citrix Cloud Control plane geo-selection or the location of the applications being accessed. Configuration, such as authorization meta-data is replicated to all PoPs.

Logs used by Citrix® for diagnostic, monitoring, business, and capacity planning are secured and stored in one central location.

Customer configuration is stored in one central location and distributed globally to all PoPs.

Data flowing between the cloud and customer premises uses secure TLS connections over port 443.

Encryption keys used for user authentication and single sign-on are stored in hardware security modules.

Data isolation

The Citrix Gateway service stores the following data:

- Configuration data needed for the brokering and monitoring of the customer's applications – data is scoped by the customer when persisted.
- TOTP seeds for each user device –TOTP seeds are scoped by customer, user, and device.

Audit and Change Control

Currently the Citrix Gateway service does not make auditing and change control logs available to customers. Logs are available to Citrix which can be used to audit the activities of end-user and administrator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Credential handling

The service handles two types of credentials:

- User credentials: End-user credentials (passwords and authentication tokens) might be made available to the Citrix Gateway service to perform the following:
  - Citrix Secure Private Access - The service uses the user's identity to determine access to SaaS and Enterprise web applications and other resources.
  - Single sign-on - The service might have access to the user's password to complete the SSO function to internal web applications using HTTP Basic, NTLM, or forms-based authentication. The encryption protocol used for password is TLS unless you specifically configure HTTP Basic authentication.
- Administrator credentials: Administrators authenticate against Citrix Cloud. This generates a one-time signed JSON Web Token (JWT) which gives the administrator access to the management consoles in Citrix Cloud.

> **Points to note**

- All traffic over public networks is encrypted by TLS, using certificates managed by Citrix.
- Keys used for SaaS app SSO (SAML signing keys) are fully managed by Citrix.
- For MFA, the Citrix Gateway service stores the per-device keys used to seed the TOTP algorithm.
- To enable Kerberos Single Sign-On functionality, customers might configure Connector Appliance with credentials (user name + password) for a service account trusted to perform Kerberos Constrained Delegation.

Deployment considerations

Citrix recommends that users consult the published best practices documentation for deploying Citrix Gateway services. More considerations regarding SaaS apps and Enterprise web apps deployment, and network connector are as follows.

Selecting the correct Connector: The correct connector must be selected, depending on the use case:

Use Case	Connector	Form factor
User Authentication: Active Directory	Citrix Cloud Connector	Windows software
HDX Connectivity	Citrix Cloud Connector	Windows software
SaaS apps access	Citrix Cloud Connector	N/A

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use Case	Connector	Form factor
Enterprise web apps access	Citrix Cloud Connector, Citrix Connector Appliance	N/A
Enterprise apps and files delivered by Citrix Endpoint Management	Citrix Cloud Connector, Citrix Connector Appliance	N/A

Citrix Cloud Connector network access requirements

For information on Citrix Cloud Connector network access requirements, see Internet connectivity requirements.

Citrix Gateway service HDX Connectivity

Using the Citrix Gateway service avoids the need to deploy NetScaler Gateway within the customer data centers. To use the Citrix Gateway service, it is a prerequisite to use Citrix Workspace delivered from Citrix Cloud.

Customer best practices

Customers are recommended to use TLS within their network and not enable SSO for applications over HTTP.

Deprecated cipher suites

The following cipher suites are deprecated for enhanced security:

- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384
- TLS1.2-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-128-SHA256
- TLS1.2-DHE-RSA-AES256-GCM-SHA384
- TLS1.2-DHE-RSA-AES128-GCM-SHA256
- SSL3-DES-CBC3-SHA
- TLS1-ECDHE-RSA-AES256-SHA

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-DSS-AES-256-CBC-SHA
- TLS1-DHE-DSS-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-DES-CBC3-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256

Geo-location Routing

October 15, 2026

Geo-location routing allows administrators to direct user traffic to a specific region (PoPs) regardless of the user's location. Geo-location routing can be used in the following scenarios:

- **Data residency requirements:** Many countries have regulations requiring data to be stored and processed within their borders. For example, geo-location routing can be configured to ensure that all data from European Union (EU) users is routed to PoPs within the EU, complying with General Data Protection Regulation (GDPR) data residency requirements.
- **Data sovereignty:** Data is governed by the laws and regulations of the country or region where it is collected and processed. For instance, a multinational corporation can leverage geo-location routing to ensure that data from DaaS control regions like the United States, European Union, and Asia Pacific South is processed in the corresponding regional PoPs, complying with data sovereignty laws.
- **Industry-specific regulations:** Certain industry-specific regulations require data to be stored and processed in specific ways. For example, a healthcare provider can use geo-location routing to ensure that patient data is routed to Health Insurance Portability and Accountability Act (HIPAA) compliant commercial region PoPs within the United States.
- **Financial services:** Financial institutions are often subject to regulations that require financial data to be processed within specific jurisdictions. For example, a bank can use geo-location routing to ensure that transactions from Asia Pacific South customers are processed in commercial region PoPs within the Asia Pacific South, complying with local financial regulations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

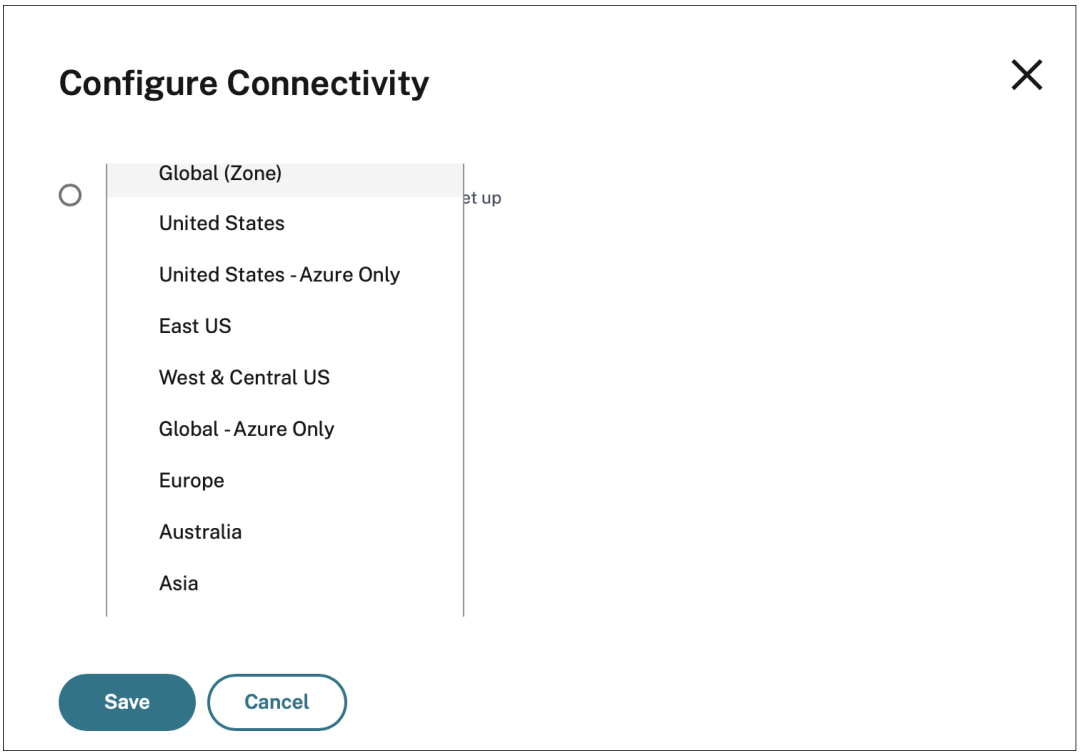
- **Traffic optimization:** Geo-location routing ensures that user traffic is directed to specific region PoPs, optimizing performance by reducing latency and improving user experience.
- **Load balancing:** By directing traffic to specific region PoPs, administrators can distribute the load across multiple PoPs, preventing overloading of any single region.

> **Note:**
>
> Geo-location routing is available only for Citrix Cloud customers in commercial regions. It is not available for Google Cloud Platform, Japan, and US Government regions.

How to configure geo-location routing in Citrix Workspace

You can configure a specific region for the user traffic from the **Resource locations** or **Workspace Configuration** page on Citrix Cloud.

1. Sign in to Citrix Cloud.
2. Click the hamburger menu and select **Resource Locations** or **Workspace Configuration**.
    a) On the **Resource Locations** page, select a location and click **Gateway**. The **Configure Connectivity** screen appears.
    b) In the **Workspace Configuration** page, in External Connectivity, select a location and click the ellipsis. The **Configure Connectivity** screen appears.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

For the list of FQDNs associated with the PoPs that support geo-location based traffic routing, see Regional FQDNs for geo-location routing.

3. In **Gateway Service Region (Optional)**, select the region to which you want to route your customer traffic.

   > **Notes**
   >
   > If you do not select any region, then **Global** is selected by default. When the region is **Global**, the traffic is diverted to the PoP that is in the closest proximity to the customer. For more information, see Optimal Gateway Routing.
   >
   > In rare scenarios, if there is an outage, and all the PoPs of a specific region are not available, then the configuration falls back to **Global** instead of blocking the traffic.

4. Click **Save**.

How to configure geo-location routing in StoreFront™

> **Important**
>
> - Geo-location routing can be configured in StoreFront only when you enable Citrix Gateway service for StoreFront. For more information, see Citrix Gateway service for StoreFront.
> - StoreFront version 2503 and later supports geo-location routing.

You can manually specify the PoP FQDN for the region you want to use. For more information on how to configure geo-location routing in StoreFront, see Add Citrix Gateway Service.

Migrate NetScaler Gateway to Citrix Gateway service for HDX Proxy

September 9, 2026

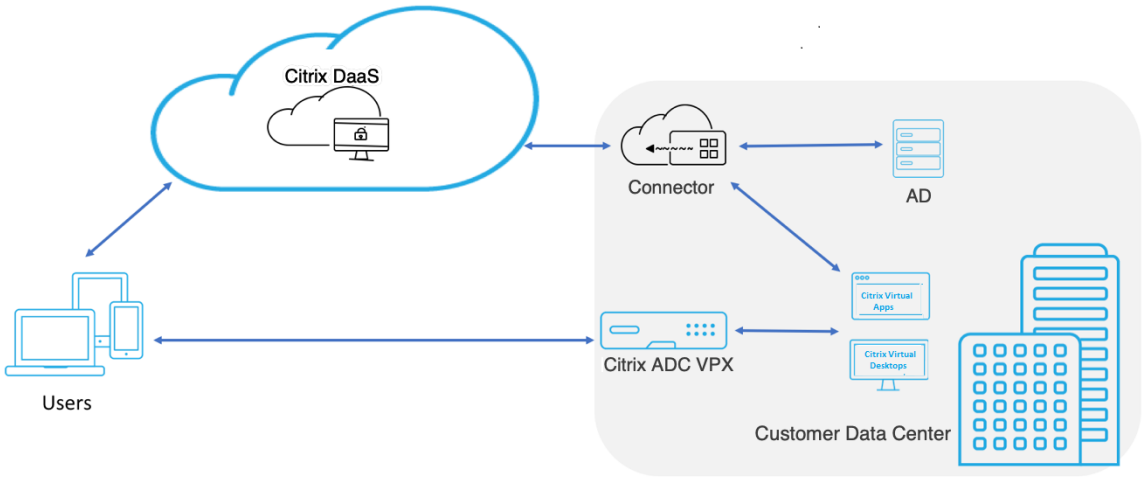
You can migrate from a Citrix Gateway for HDX Proxy and to a fully managed cloud-based HDX Proxy powered by the Citrix Gateway service on Citrix Cloud.

Cloud based HDX™ Proxy

Customers who are entitled for the Citrix DaaS get the Citrix Gateway service enabled, by default. Customers do not have to request a separate Citrix Gateway service trial.

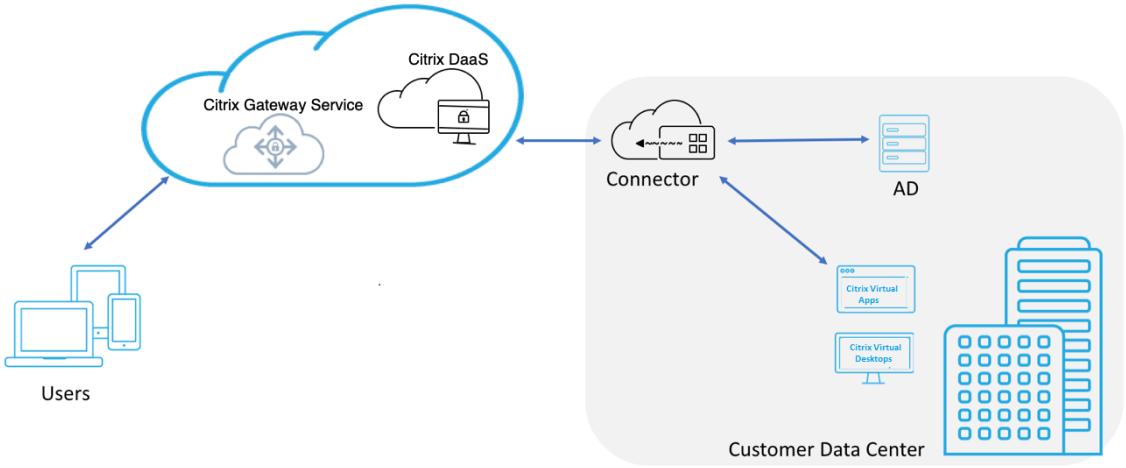
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Figure 1. Deployment with NetScaler® Gateway as HDX Proxy



Citrix Gateway service is a cloud based HDX Proxy that provides secure remote access through a cloud-based gateway that front-ends virtual apps and desktop environments that are Citrix DaaS environments.

Figure 2. Deployment with Citrix Gateway service as HDX Proxy



This feature is now included with your Citrix DaaS and Workspace Service entitlements. You can enable this feature.

Migration from an on-premises NetScaler Gateway to cloud based Citrix Gateway service

The NetScaler Gateway appliance is customer managed and cloud based Citrix Gateway service is Citrix managed. This section explains how to migrate from an on-premises NetScaler Gateway to cloud-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

hosted Citrix Gateway service for HDX Proxy. Though NetScaler Gateway and Citrix Gateway service provide HDX Proxy, the underlying infrastructure and working mechanism is different. However, the steps to enable HDX Proxy on cloud is simple and straight forward with just a few clicks.

To enable this migration, enable the Citrix Gateway service for Citrix DaaS. Once enabled, traffic starts traversing through the Citrix Gateway service and an on-premises NetScaler Gateway is no longer required.

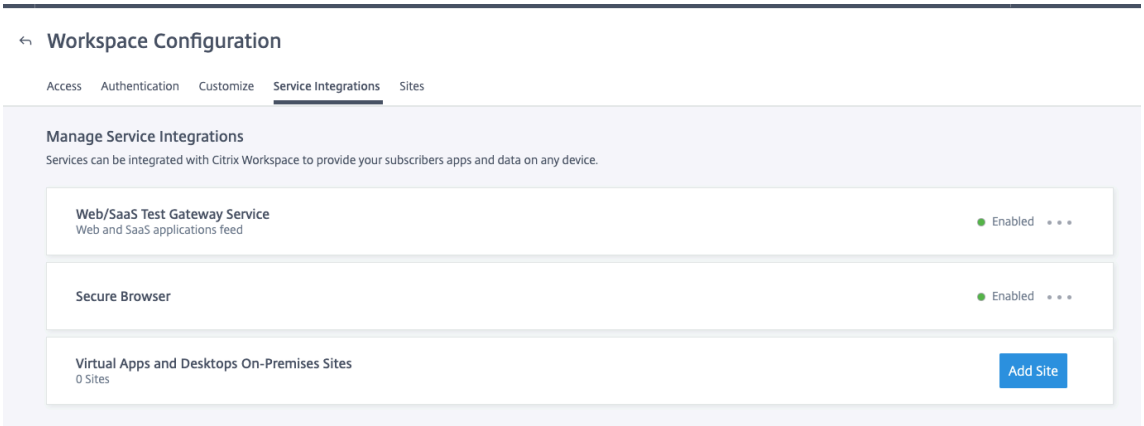
Following are the assumptions made before you begin migration from an on-premises NetScaler Gateway to cloud based Citrix Gateway service.

- The customer has subscribed for Citrix Cloud Service and has purchased Citrix DaaS.
- The customer uses an on-premises Active Directory to authenticate users on cloud.

Enable the Citrix Gateway service

Following are the steps to enable Citrix Gateway service for Citrix DaaS users:

1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon and choose **Workspace Configuration**.
3. Click **Service Integrations**.
4. Locate the ellipsis next to **Gateway**, click the ellipsis, and then click **Enable**.

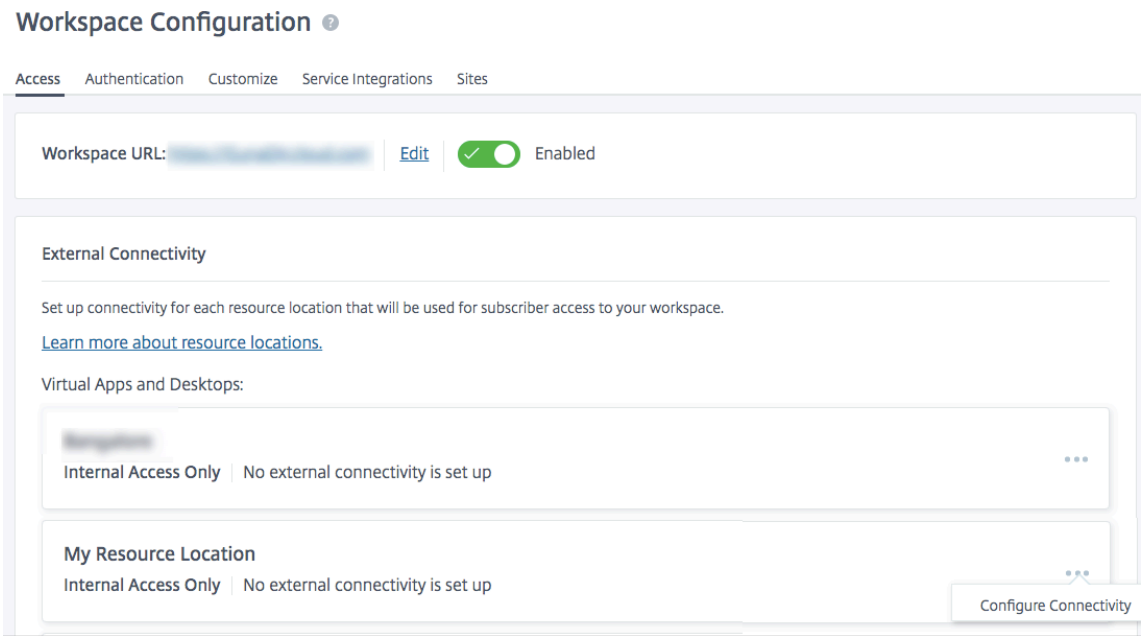


Following are the steps to enable the Citrix Gateway service for Citrix Workspace users.

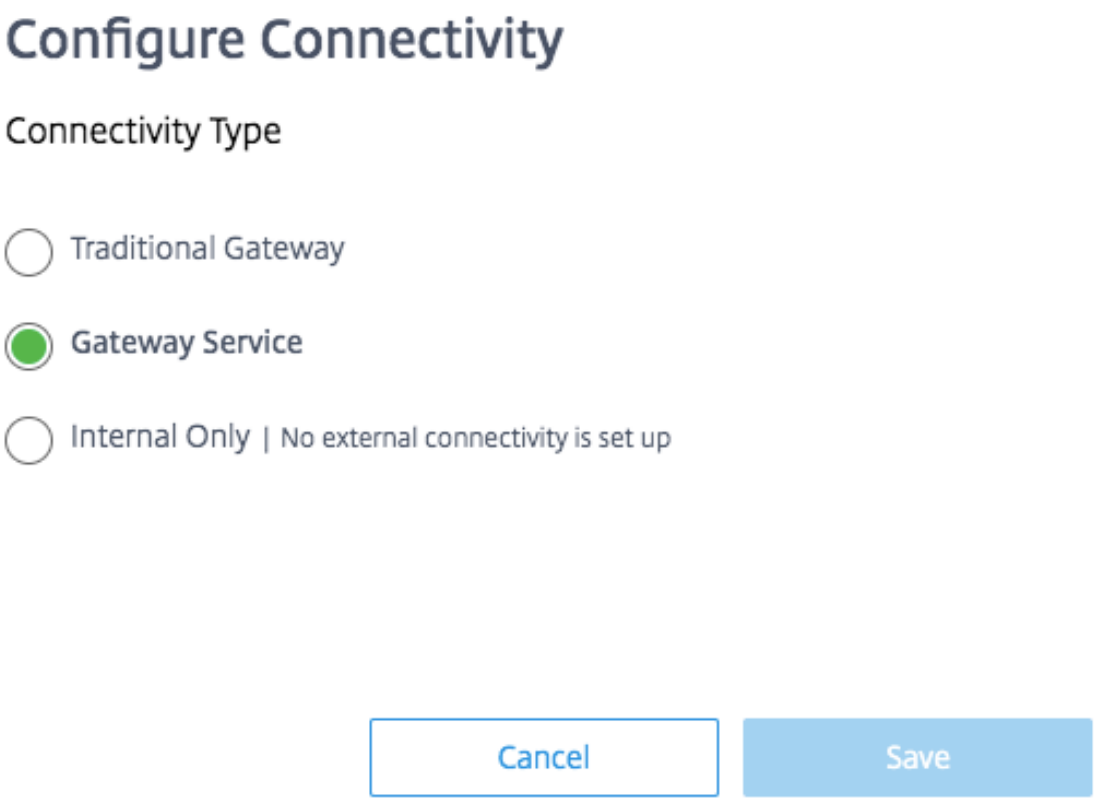
1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon and choose **Workspace Configuration**.
3. In the **Access** tab, under **External Connectivity** section, locate the ellipsis next to **My Resource Location** under **Citrix DaaS**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click the ellipsis, click **Configure Connectivity**.



5. Choose **Citrix Gateway service** in the pop-up window and then click **Save**.

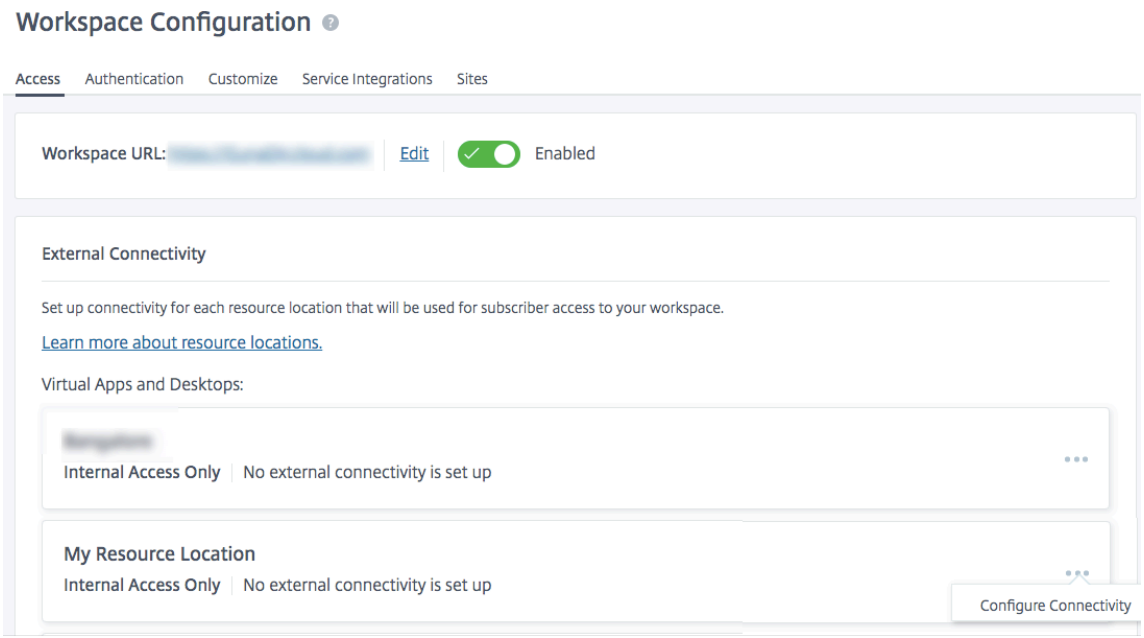


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Roll back to NetScaler Gateway

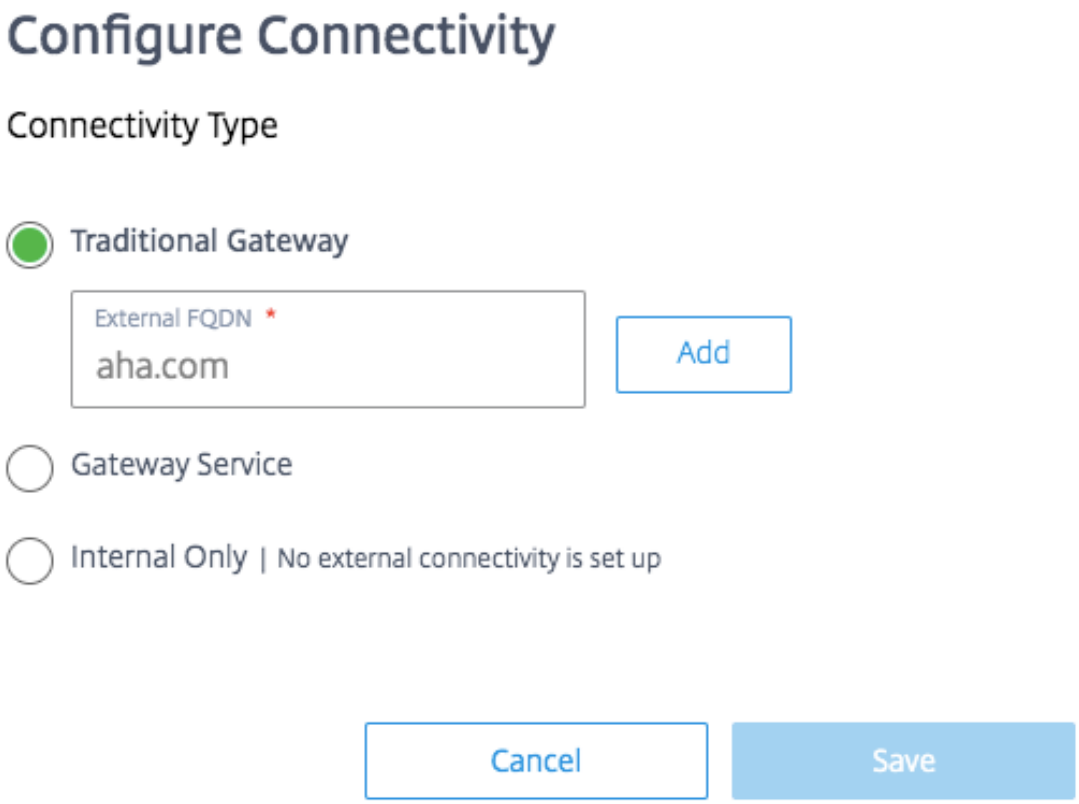
To roll back the HDX Proxy to an on-premises NetScaler Gateway, perform the following.

1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon on the top left and choose **Workspace Configuration.**
3. In the **Access** tab under **External Connectivity** section, locate the ellipsis next to **My Resource Location** under **Citrix DaaS**.



4. Click the ellipsis, click **Configure Connectivity**.
5. Choose **Traditional Gateway** and enter the FQDN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Click **Add** and then click **Save**.

HDX Adaptive transport with EDT support for Citrix Gateway service

September 30, 2026

Enlightened Data Transport (EDT) is a Citrix-proprietary transport protocol built on top of UDP. EDT delivers a superior user experience on challenging long-haul connections while maintaining server scalability.

Adaptive Transport is a data transport mechanism for Citrix Virtual Apps and Desktops. Adaptive Transport provides the ability to use EDT as the transport protocol for ICA, and switch to TCP when EDT is not available.

For more information on Adaptive Transport and EDT, see the Adaptive Transport documentation.

Prerequisites

- Citrix DaaS
- Virtual Delivery Agent (VDA) 2012 or later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Workspace app
  - Windows: version 1912 or later (2105 or later recommended)
  - Linux: version 1912 or later (2104 or later recommended)
  - Mac: version 1912 or later
  - iOS: latest version available in the Apple App Store
  - Android: latest version available in Google Play
- UDP port 443 must be allowed for outbound traffic from VDA to Citrix Gateway service
- The rendezvous protocol must be enabled and working. For details, see the Rendezvous Protocol documentation.
- Ensure that Adaptive Transport is enabled. For details, see the Adaptive Transport setting documentation.
- For more information on Adaptive Transport and EDT, see the Adaptive Transport documentation.

Considerations

The following are some of the considerations for using EDT with the Citrix Gateway service.

- It is highly recommended to enable EDT MTU Discovery. For details, see the Adaptive Transport documentation.
- EDT with Citrix Gateway service is only available when using Rendezvous. If HDX sessions are being proxied through the Cloud Connector, only TCP is available for data transport.
- When an EDT session establishment fails the session falls back to TCP, causing an increase in the session launch time.
- If you want to continue to proxy HDX™ sessions through the Cloud Connector, consider disabling Adaptive Transport via the Citrix Studio policy to avoid the potential increase in session launch times introduced by the fallback sequence.
- Citrix recommends using EDT through the Citrix Gateway service only with VDAs running on Windows 10 and Windows Server 2019. There are limitations on Windows Server 2012 R2 and 2016 that do not allow for an MTU greater than 1024 for DTLS-encrypted sessions, which can affect the performance and user experience.
- With Adaptive Transport, Citrix Gateway service does not Support UDP Audio.

Transport protocol validation

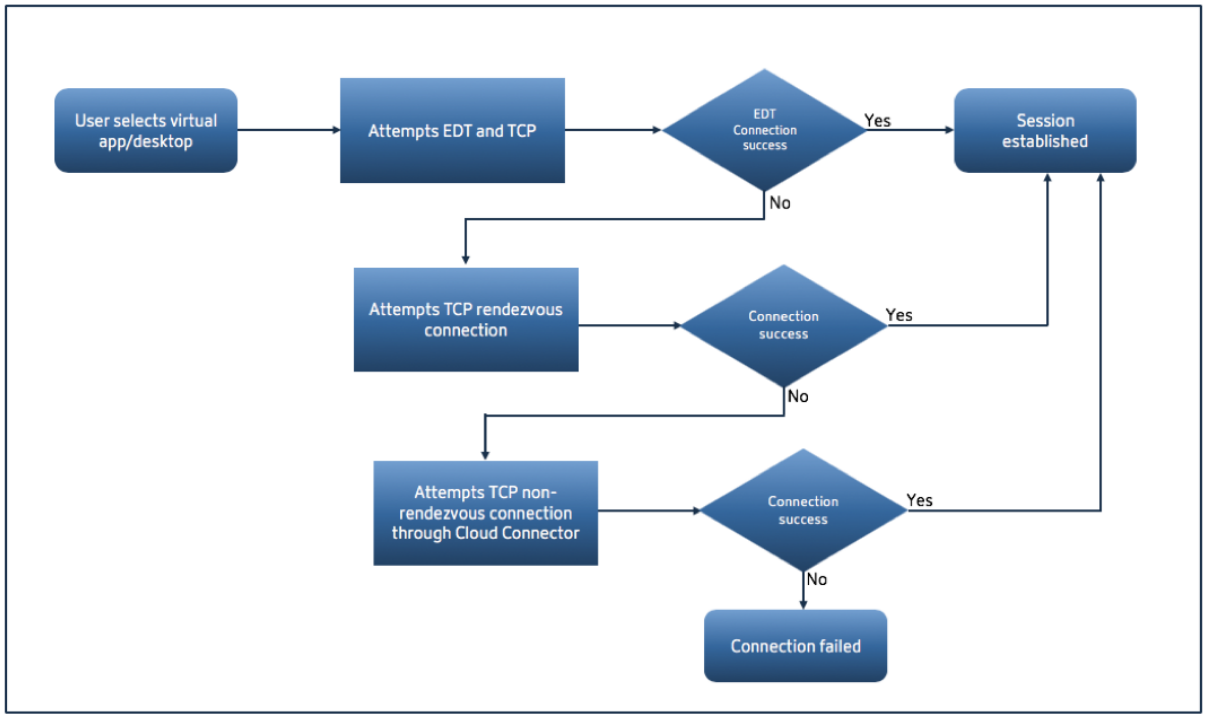
To know if your sessions are using EDT, refer to the following:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Connection protocol in Citrix Director: CTX220730.
- After you launch an app or a desktop, go to **Citrix Workspace app > Connection Center**, select the appropriate session, click **Properties**, and look at the Transport encryption property. If it shows DTLS, the session is using EDT for transport. If it shows TLS, the session is using TCP for transport.
- If you launched a desktop, you can open a PowerShell or command prompt and run "`ctxsession -v`". The Transport Protocols property displays the connection method being used:
  - EDT Rendezvous: "**UDP > DTLS > CGP > ICA®**"
  - TCP Rendezvous: "**TCP > SSL > CGP > ICA**"
  - Proxy through Cloud Connector: "**TCP > CGP > ICA**"

Connection fallback

If EDT negotiation fails for any reason, the session falls back to TCP with Rendezvous. And if that fails, then the session falls back to proxying through the Cloud Connectors.



EDT MTU discovery

It is highly recommended to enable EDT MTU Discovery to ensure that each session uses the optimal MTU for that connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In case EDT MTU Discovery is disabled or the user's client does not support the feature, the EDT MTU is automatically set to 1380 to avoid fragmentation-related issues.

It is possible for users to connect via a network that requires an MTU lower than 1380, which is mostly seen with mobile networks (3G, 4G) or VPN connections. If this is the case in your environment, and the clients in use by the users do not support EDT MTU Discovery, Citrix recommends that you disable Adaptive Transport until the feature is available in your target client platform.

For more details on EDT MTU Discovery, see Adaptive Transport documentation.

Troubleshooting

The following provides some general troubleshooting guidance.

Sessions connect but are not using EDT:

1. If the sessions are being proxied through the Cloud Connector, make sure that Rendezvous is enabled and that it works properly, as this is a pre-requisite for using EDT with the Citrix Gateway service. For details, see the Rendezvous documentation.
2. If the sessions are using TCP Rendezvous:
    - Make sure you are using VDA version 2012 or later.
    - Check whether Adaptive Transport is enabled in Citrix policies.
    - Make sure that the appropriate firewall rules are in place to open UDP 443 from the VDA machines to the Citrix Gateway service. For more details, see the Rendezvous](/en-us/citrix-virtual-apps-desktops-service/hdx/rendezvous-protocol.html) documentation.
    - If there is a local firewall enabled in the VDA machine (for example Windows Defender Firewall), make sure that there are no rules blocking UDP 443.
    - If using a proxy, only SOCKS5 proxies can be used to proxy EDT. For details, see the Rendezvous documentation.

Sessions connect with EDT but disconnect randomly after some time:

1. Make sure you are using VDA version 2012 or later.

Session fails to connect:

1. Make sure you are using VDA version 2012 or later.
2. If using a client that supports EDT MTU Discovery, ensure that EDT MTU Discovery is enabled. This helps mitigate fragmentation-related issues. For details, see Adaptive Transport documentation.
3. If using a Linux or Android client:
    - Check if Windows or Mac clients are working properly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Check if the CWA version is upgraded to Linux 2104, Android 21.5.0 or later.
- If you are using an older version of CWA then disable Adaptive Transport and ensure that TCP Rendezvous works properly.
- Once TCP Rendezvous works, if the session fails to connect after re-enabling Adaptive Transport, see the troubleshooting steps mentioned in step **Sessions connect but are not using EDT > If the sessions are using TCP Rendezvous**.

Network metrics monitoring for Citrix Gateway service

September 9, 2026

Network metrics monitoring for Citrix Gateway service enables administrators to view session details, latency breakdowns, and other key network metrics. This enables effective troubleshooting and remediation of HDX sessions, including latency breakdowns across hops, a capability previously unavailable to customers. The network metrics provide admins a complete visibility into HDX traffic flowing between the Citrix Workspace app, Virtual Delivery Agent (VDA), and Citrix Gateway service.

Supported platforms and versions

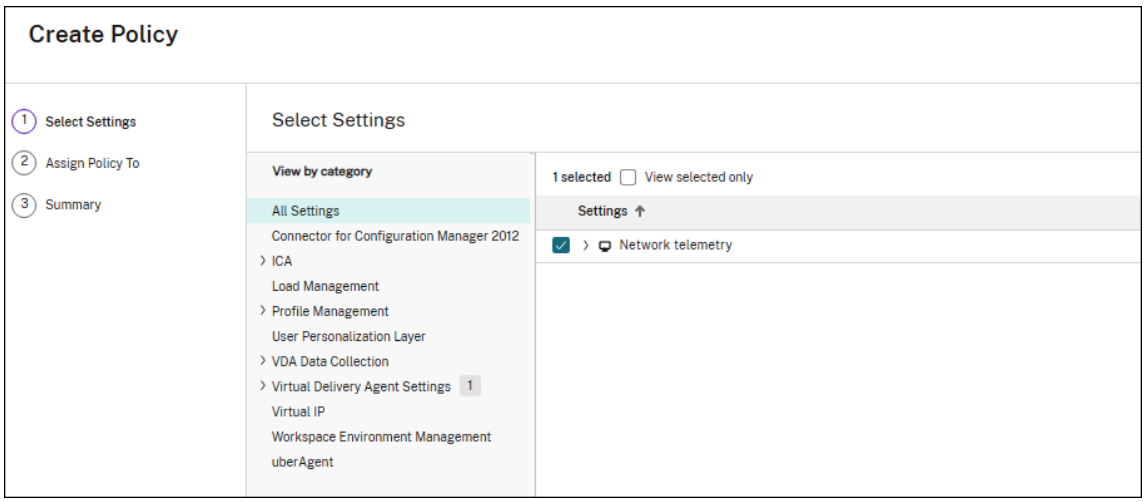
The following table lists the platforms and the versions that support network metrics monitoring:

Component	Platform	Supported version
Citrix Workspace app	Windows	2411 or later
Citrix Virtual Apps and Desktops	Windows	2411 or later

Prerequisites

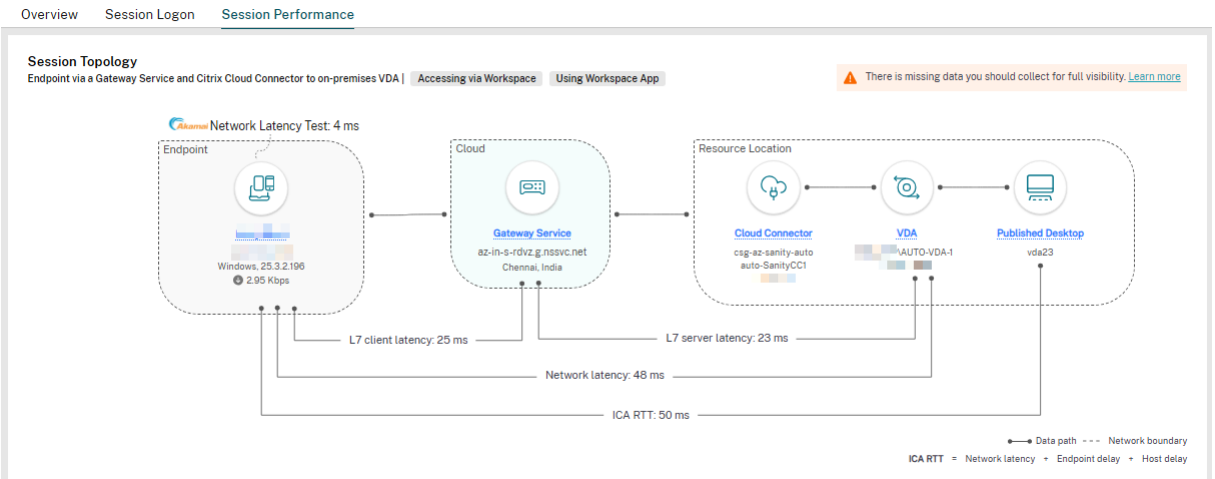
- Admin must enable the **Network telemetry** policy in Citrix Studio or Web Studio. For more information, see Create policies.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Monitor the network metrics for Citrix Gateway service in DaaS Monitor

In DaaS Monitor, the **Session Performance** tab provides a visual representation of network metrics, enabling administrators to access real-time latency data, historical reports, and comprehensive performance insights for troubleshooting. The availability of both real-time and historical data supports various use cases for customers using Citrix Gateway service. For more information, see Diagnose Session Performance issues.



Troubleshooting performance issues using network metrics

The following table provides a list of network metrics that the admin can monitor in DaaS Monitor to diagnose performance issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network Metrics	Description
Client side retransmits	Indicates the number of packets retransmitted between the PoP and the user's endpoint. A high value of this metric indicates high bandwidth utilization or link issues.
ICA® RTT	High RTT indicates network congestion or distance-related delays and impacts user experience.
Jitter	High jitter leads to inconsistent performance and smoothness of applications.
L4 metrics	For the list of L4 metrics, see Current/Terminated Sessions Report.
Layer 4 client-PoP latency Layer 4 PoP-server latency	Indicates which network hop in the session contributes to the most delay, helping the admin to focus more on that area.
L7 client latency	Indicates the L7 layer latency (application-level processing time, the seventh layer on OSI model) measured using ICA probes and responses sent between Citrix Workspace™ app and the host on client side.
L7 server latency	Indicates the L7 layer latency (application-level processing time, the seventh layer on OSI model) measured using ICA probes and responses sent between Citrix Workspace app and the host on server side.
Network latency	Indicates the breakdown of the network latency, which can be compared to ICA latency and ICA RTT for isolation of issues.
QoS	Indicates the amount of packet loss in percentage. Even small amounts of loss can degrade performance significantly.
Server side retransmits	Indicates the number of packets retransmitted between the PoP and the back-end server (VDA). A high value of this metric indicates a network issue within the data center.
Throughput (bps)	Indicates network bandwidth used. High utilization indicates congestion and bottlenecks. **Note:** Only for rendezvous, the VDA might have server retransmits.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Benefits

The visual representation of network metrics offers the following benefits, helping administrators effectively troubleshoot issues in HDX™ sessions:

- Reduce the mean time to resolve (MTTR).
- Reduce support costs with minimized escalations.
- Unified troubleshooting experience for HDX session performance.

Key features

- **Comprehensive insights:** Admins receive detailed network metrics, aiding in analysis, informed decision-making, and proactive issue resolution.
- **L7 latency monitoring:** To improve network diagnostics, the enhanced network metrics monitoring allows Citrix Gateway service to calculate the L7 latency for each of the following hops:
  - First hop or front-end hop from Citrix Workspace to Citrix Gateway service.
  - Second hop or back-end hop from Citrix Gateway service to VDA.

  The L7 latency monitoring enables the admin to identify and resolve the performance issues by monitoring application-level processing time.
- **Transport layer independence:** The network metrics monitoring for Citrix Gateway service happens consistently independent of the transport layer in use (TCP and EDT).
- **Data security:** TLS/DTLS encryption ensures that the network metrics are transmitted securely over the internet, maintaining confidentiality and integrity.

Citrix Gateway service on Google Cloud Platform

October 15, 2026

With Citrix Gateway service support on the Google Cloud Platform (GCP), customers running their workloads on Google Cloud can take advantage of Google Cloud's high-performing global network using the Citrix Gateway optimal routing feature. The optimal gateway routing feature directs clients to the closest GCP Citrix Gateway service POP. Also, the Citrix Gateway service on Google Cloud provides secure connectivity between Citrix Workspace clients and virtualization resources to deliver sessions with the lowest latency and the best user experience possible.

Currently, Citrix Gateway service for GCP is available in the following regions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- United States
  - Los Angeles
  - Oregon
  - South Carolina
- Europe
  - London
  - Zurich

> **Note:**
>
> - GCP POPs are only available for Citrix DaaS customers who have purchased subscriptions from the Google Cloud Marketplace and running their workloads on Google Cloud.
> - Citrix Gateway service account - Customers who are entitled for Citrix DaaS get the Citrix Gateway service enabled, by default. Customers do not have to request a separate Citrix Gateway service trial. For details, see Sign up for the service.

Prerequisites

- Citrix Cloud account. For details see, Sign up for Citrix Cloud.

Citrix Gateway service features supported

The following are some of the features supported by the Citrix Gateway service for GCP.

TCP HDX™ Proxy - Currently, only TCP HDX Proxy is supported. Virtual Apps and Desktops launch is supported only via the TCP protocol.

Rendezvous V1 - When using the Citrix Gateway service, the Rendezvous protocol version V1 allows VDAs to bypass the Citrix Cloud Connectors to connect directly to gateway POP for data-path traffic. For details, see Rendezvous V1.

Rendezvous V2 - The Rendezvous protocol version V2 supports bypassing the Citrix Cloud Connectors for both control traffic and HDX session traffic. For details, see Rendezvous V2.

> **Important:**
>
> EDT support is not yet enabled for GCP.

How to enable Citrix Gateway service

Customers who are entitled for Citrix DaaS get the Citrix Gateway service enabled, by default. Customers do not have to request a separate Citrix Gateway service trial. For details, see Sign up for the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

service.

Limitations

Currently, GCP in available only in the United States and Europe regions. GCP customers from other regions might observe high latency issues.

References

- Citrix Cloud Connector connectivity requirements –For details, see Cloud Connector common service connectivity requirements.
- Scale and size considerations for Cloud Connectors. For details, see Scale and size considerations for Cloud Connectors.

Support for Citrix Virtual Apps and Desktops

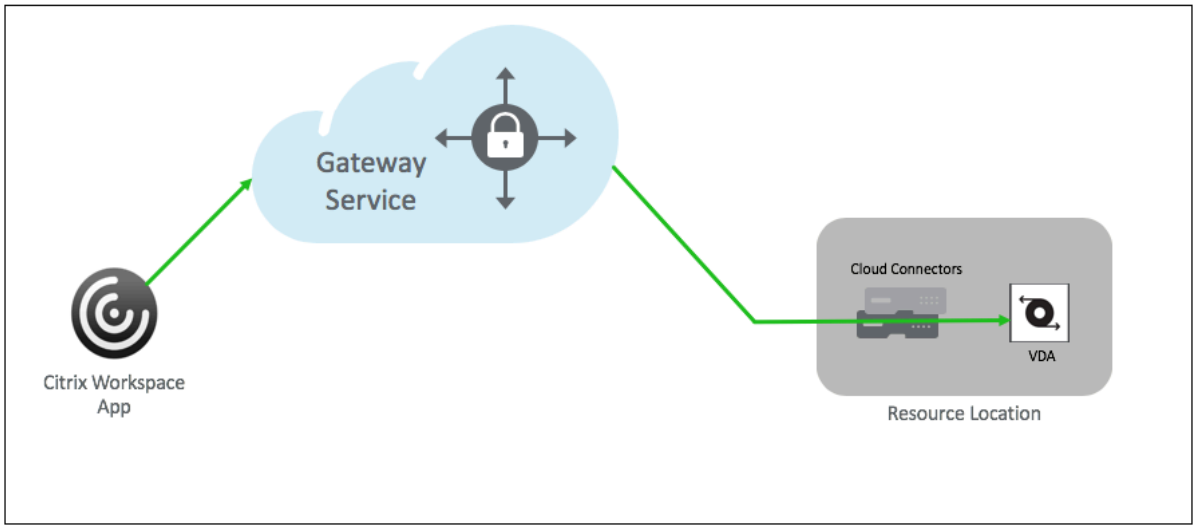
September 30, 2026

Citrix Gateway service provides users with secure access to Citrix Virtual Apps and Desktops across a range of devices including laptops, desktops, thin clients, tablets, and smartphones.

Citrix Gateway service enables secure, remote access to Citrix Virtual Apps and Desktops, without having to deploy NetScaler Gateway in the DMZ or reconfigure your firewall. The entire infrastructure overhead of using Citrix Gateway moves to the cloud and hosted by Citrix.

You enable Citrix Gateway service in Citrix Cloud. After enabling the service, users can access their VDAs from outside their network, as shown in the following diagram.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



How it works

Users' endpoints and their on-premises hosted resources VDAs are connected to their nearest respective POPs through Citrix Cloud Connectors. Later, when users select a virtual app or desktop to launch from their Workspace app, the nearest POP hosting that connection identifies the pertinent resource location and directs it to establish a Citrix Cloud Connector session to that POP forming an end-to-end connection and then a virtual session is established.

- Sessions are linked through Citrix Gateway service across cloud partner's WANs.
- VDAs and Workspace endpoints rendezvous at the Citrix Gateway service POP closest to the user.
- High quality sessions.

For more details, see Citrix Gateway service for HDX Proxy.

Citrix Gateway Service for StoreFront

September 9, 2026

> **Important information:**
>
> - Citrix Gateway service for StoreFront is available in the Citrix DaaS environments and on-premises Citrix Virtual Apps and Desktops.
> - This document describes the steps that you can perform to deploy Citrix Gateway service for StoreFront in a scenario where you prefer to use the on-premises NetScaler Gateway for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> authentication and on-premises StoreFront for enumeration.
> - Citrix Gateway service for StoreFront is not supported in Citrix Cloud Japan and Citrix Cloud Government environments.

Overview

Citrix Gateway service for StoreFront is a cloud-based HDX solution that provides secure remote access to resources accessed from on-premises StoreFront. You can leverage the scalability and reliability of Citrix Cloud (for HDX proxy) without changing your on-premises StoreFront and on-premises NetScaler Gateway environments.

Consider that you are a Citrix DaaS customer using on-premises StoreFront as your enterprise application store and on-premises NetScaler Gateway for remote access. If you are looking for an option to leverage a cloud-hosted remote access solution (HDX proxy) while maintaining on-premises StoreFront as your user portal and on-premises NetScaler Gateway for authentication, Citrix Gateway service for StoreFront is for you.

Citrix Gateway service handles the HDX proxy launches using a Windows-based Cloud Connector in your resource location.

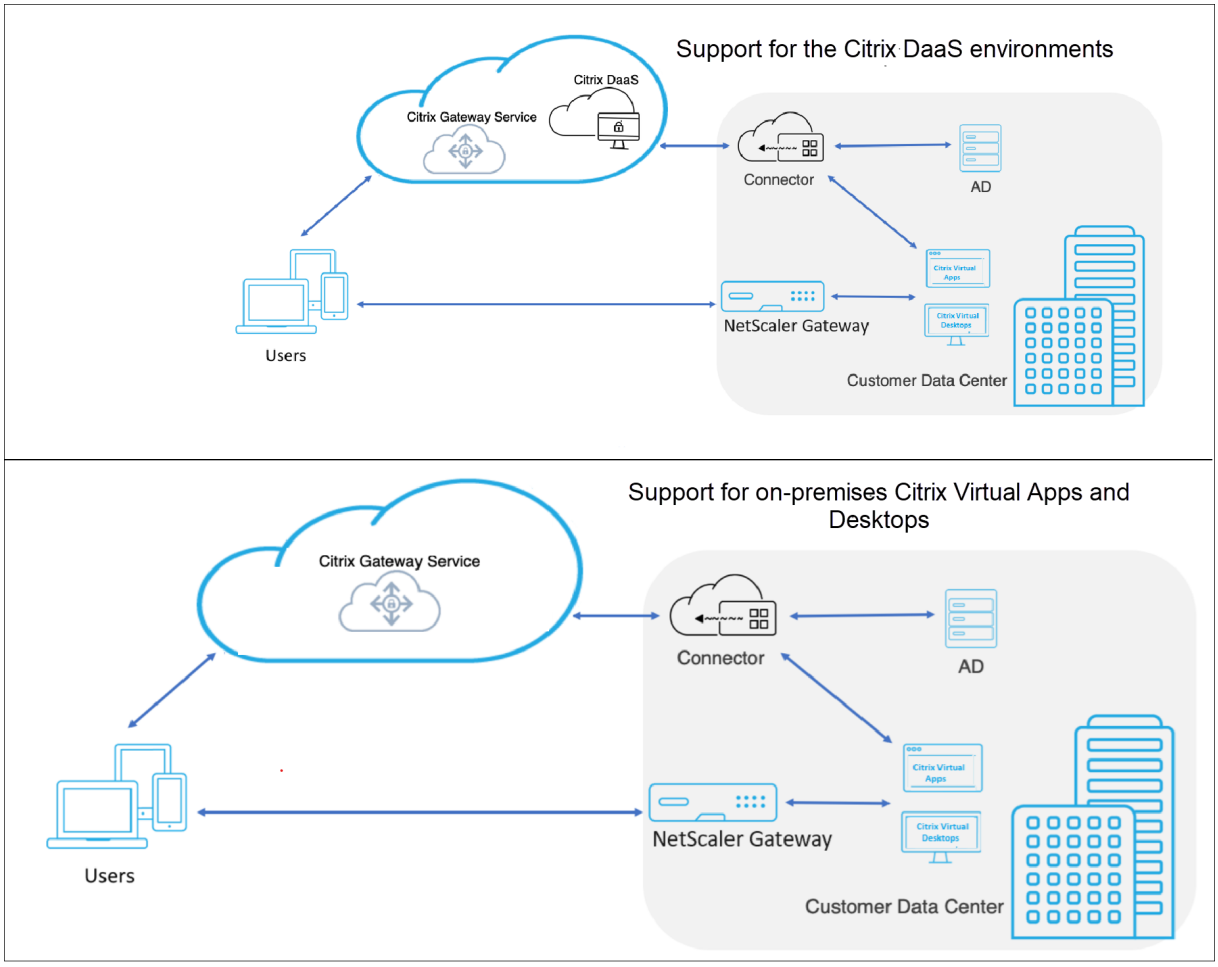
Citrix Gateway service for StoreFront supports the following use cases:

- HDX over TCP/EDT
- Local Host Cache (LHC) for resiliency
- Rendezvous V1

The following use cases are not supported:

- Non-HDX™ use cases such as RDP proxy, VPN, PC over IP (PCoIP).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Benefits

- Citrix DaaS customers can use their existing on-prem NetScaler Gateway URL.
- Ensures high resiliency because of the multi-cloud and multi-geo architecture of Citrix Gateway service.
- HDX proxy performance and scale requirements are now managed by Citrix Gateway service. They are no longer customer-managed.

Prerequisites

- Use NetScaler 13.1 version or later. For details, refer to the NetScaler documentation.
- To use Citrix Gateway service for StoreFront in Citrix DaaS environments, use an on-premises StoreFront version 2407 or later. For geo-location routing, use StoreFront 2503 or later. For details, refer to StoreFront System requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To use Citrix Gateway service for StoreFront in on-premises Citrix Virtual Apps and Desktops, use Citrix Virtual Apps and Desktops version 2503 and later.
- Onboard to Citrix Cloud and install Citrix Cloud Connector (Desktop Delivery Controller for Citrix DaaS outages. STA for ticketing).

  You can use an existing Cloud Connector or deploy a new one. If your connector upgrade is disabled, contact Support to get it enabled.

  For details about the Citrix Cloud Connector requirements, see Citrix Cloud Connector requirements. For details about the sizing requirements, see Size and scale considerations for Cloud Connectors.

> **Note:**
>
> Only a Windows-based Cloud Connector is supported. Connector Appliance is not supported.

Resiliency with Local Host Cache (LHC)

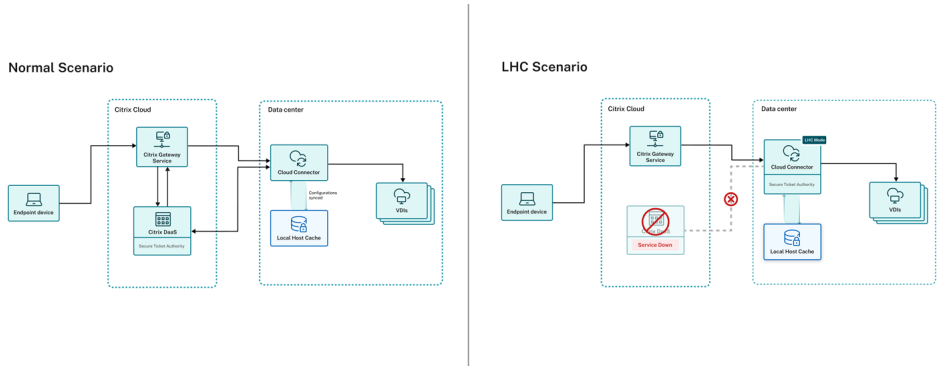
Local Host Cache (LHC) is a functionality of Citrix DaaS that enables users to continue accessing apps and desktops when Cloud Connectors lose connectivity with Citrix Cloud.

When using Gateway Service with StoreFront, the STA ticket redemption behavior differs between working normally and being in LHC mode.

- When working normally, STA tickets are redeemed from the ticketing service hosted in Citrix Cloud.
- When in LHC mode, STA tickets are redeemed from the Cloud Connector.

> **Note:**
>
> Cloud Connectors must maintain connectivity with the Gateway Service in LHC mode to redeem STA tickets. Launches fail in LHC mode if connectors cannot communicate with the Gateway Service.

The following diagram illustrates how STA ticket redemption works in a Citrix Gateway service for StoreFront deployment in a normal working scenario and when in LHC mode.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

References

- Citrix Gateway service for StoreFront Deployment - Tech Zone Article
- Citrix Gateway service for StoreFront - GA Blog
- Citrix Cloud Connector requirements
- Local Host Cache support for Citrix DaaS
- Launch ICA file logging
- Session launch
- Support

Known issues and limitations

- If you have opted for Citrix Gateway service for StoreFront preview with StoreFront 2311 or 2402 and you have configured a Gateway Service for HDX instance, the configuration becomes invalid with StoreFront 2407. Delete the existing gateway instance and create instances.

Upcoming enhancements

The following enhancements are planned in the upcoming releases:

- Session Performance - L7 Latency breakdown

FAQ

What is the Citrix Gateway service for StoreFront?

Citrix Gateway service for StoreFront is a cloud-based HDX solution. It enables customers to maintain their existing access tier and authentication infrastructure (NetScaler and StoreFront) while leveraging the benefits of a cloud-based HDX Proxy solution (Citrix Gateway service)

What are the benefits of using Citrix Gateway service for StoreFront?

The benefits include the following:

- Flexibility: You can retain your existing Citrix NetScaler and StoreFront servers. Citrix Gateway service is seamlessly integrated with these components to enable access to virtual apps and desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Scalability: As Citrix Gateway service is hosted in the cloud, it can be easily scaled up or down as per the requirement.

Is Citrix Gateway service for StoreFront a fully managed service?

No, Citrix Gateway service for StoreFront is a solution that helps offload the HDX Proxy from customer-managed NetScaler to Citrix-managed Gateway Service.

Do I need to re-architect my access tier to use Citrix Gateway service for StoreFront?

No, Citrix Gateway service for StoreFront allows you to maintain your existing access tier and authentication infrastructure.

What security measures are in place to protect my data and applications?

Citrix Gateway service for StoreFront employs robust security measures to ensure the security and integrity of your data and applications. See Technical Security

How does the Citrix Gateway service for StoreFront handle scalability and high traffic volumes?

Citrix Gateway service for StoreFront is designed to handle high traffic volumes and scale to meet the needs of large enterprises, ensuring uninterrupted access to applications and data. See CGS PoPs.

What support options are available for Citrix Gateway service for StoreFront?

Citrix offers comprehensive support options, including documentation, training, and technical support, to ensure the successful deployment and operation of Citrix Gateway service for StoreFront.

Can I use Citrix Gateway service for StoreFront with other Citrix products and services?

Yes, Citrix Gateway service for StoreFront is designed to integrate seamlessly with other Citrix products and services, including Citrix Workspace, Citrix Virtual Apps and Desktops, and Citrix Hypervisor.

How is Citrix Gateway service for StoreFront licensed and priced?

All Universal HMC, CPL, and existing DaaS Customers are entitled to use Citrix Gateway service for StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Do I need to upgrade the CVAD components also to 2407 or later?

No, there is no need to upgrade the CVAD components to 2407. Only StoreFront upgrade to 2407 is required.

I am a DaaS customer with CVAD on-premises sites. Will I be able to use this solution now?

Future enhancements will include support for customers with separate Citrix Virtual Apps and Desktops sites alongside their Citrix DaaS deployments. This will help offload the HDX proxy for on-premises sites and ensure consistency across the deployment.

Support for the Citrix DaaS environments

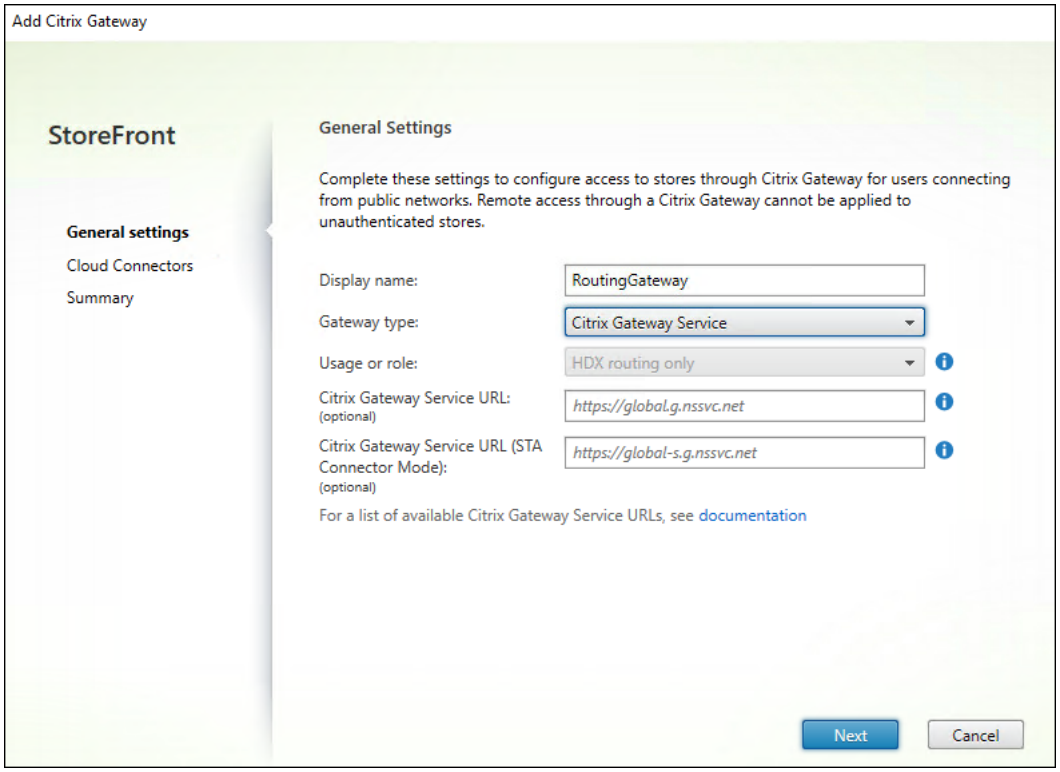
September 9, 2026

The Citrix Gateway service for StoreFront supports the Citrix DaaS environments. It is assumed that you already have an on-premises NetScaler Gateway. You can continue to use the same gateway for authentication and remote access to your StoreFront store. You can also use the same gateway to provide HDX routing to a subset of resources, such as those hosted by a Citrix DaaS deployment which Citrix Gateway service does not support. For more details on configuring NetScaler Gateway, see the StoreFront documentation.

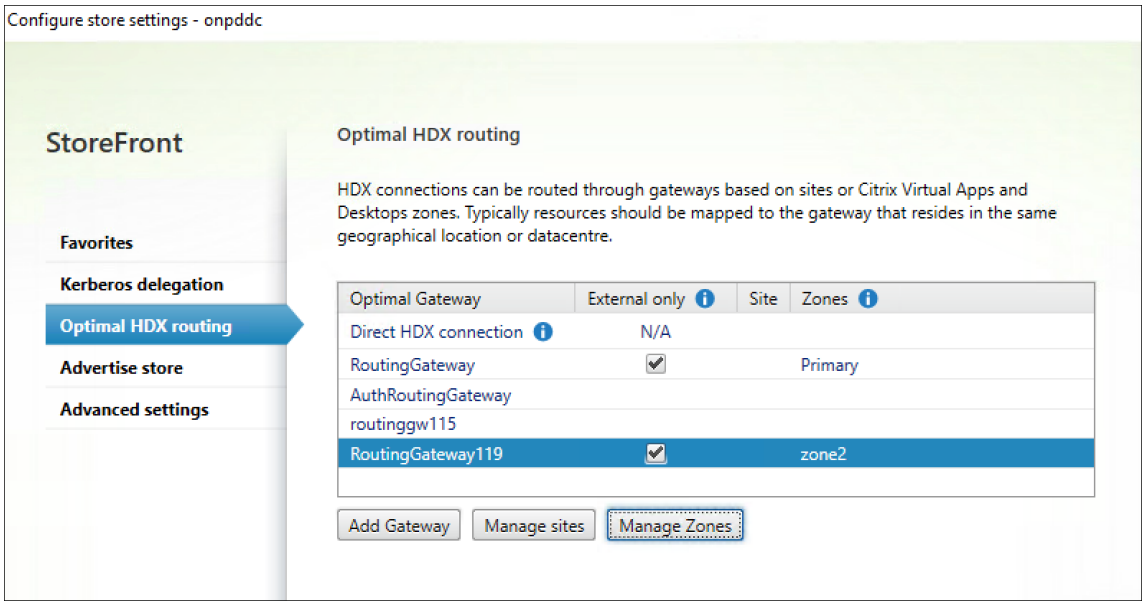
To configure Citrix Gateway service for HDX routing for some or all of your resources, create a gateway in StoreFront, and then use the Optimal Gateway Routing functionality of StoreFront to configure when it needs to be used:

1. Configure a gateway of type **Citrix Gateway Service** within StoreFront. Normally a single gateway is sufficient. However if you wish to use different geo-location rules for different sites or zones then you can configure multiple gateways with different gateway service URLs. For more information, see Add Citrix Gateway Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Choose for which sites or zones you wish HDX connections to be routed via those gateways. For more information, see Optimal HDX routing.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support for on-premises Citrix Virtual Apps and Desktops

October 15, 2026

The Citrix Gateway service can be used with on-premises deployments of StoreFront and Citrix Virtual Apps and Desktops. You can continue to use your on-premises NetScaler Gateway and StoreFront for authentication, authorization, and enumeration. Citrix Gateway service is used to launch virtual apps and desktops for all or some regions. This approach maximizes the value of existing remote access infrastructure and minimizes administrative effort. This is particularly useful for providing remote access to workloads in satellite locations where you do not have a StoreFront server, thereby completely removing the need for a NetScaler Gateway in that location.

Key benefits

The integration of Citrix Gateway service with on-premises sites offers the following benefits:

- **Customization retention:** NetScaler Gateway and StoreFront™ customizations can be retained, ensuring a consistent user experience.
- **Minimized maintenance:** HDX proxy performance and scale requirements are now managed by Citrix Gateway service, eliminating the need for customer management.
- **Existing URL:** DaaS customers can continue using their familiar on-premises NetScaler® Gateway URL.
- **Leveraging LHC for enhanced resiliency:** Local Host Cache (LHC) supports resiliency needs by allowing the connector to function as a local Secure Ticket Authority (STA) during outages.
- **Better user experience:** Ability to use geographically closer PoPs reduces latency and improves performance.
- **High resiliency:** Ensures high resiliency because of the multi-cloud and multi-geo architecture of Citrix Gateway service.

Prerequisites

1. You must have a functional on-premises working environment where NetScaler Gateway is used for authentication and authorization and StoreFront is used for enumeration.
2. Upgrade StoreFront to version 2503 or higher. For more information, see Upgrade StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a resource location on Citrix Cloud™

1. Onboard to Citrix Cloud. For more information, see Create a Citrix Cloud account and Connect to Citrix Cloud.
2. On Citrix Cloud, install Cloud Connectors and associate them with the resource location. For more information, see Cloud Connector Installation.

> **Note:**
>
> To make your existing apps and desktops available to subscribers, add your site (Citrix Virtual Apps and Desktops deployment) to Citrix Workspace. For more information, see Aggregate Virtual Apps and Desktops in workspaces.

Configure the resource location and policies on the on-premises Delivery Controller™

1. Run the following command on the Windows Active Directory (AD) or Domain Controller (DC) server, to retrieve the Security Identifiers (SIDs) of connector machines in a Windows AD or DC environment. Note the SIDs of the connector machines.

```
Get-ADComputer -Filter * | Select-Object Name, SID
```

2. In the on-premises Delivery Controller, create a zone and map it to the resource location created in Citrix Cloud.

   a) In on-premises Delivery Controller, run the following command in the PowerShell and note the Uid generated for the required resource location:

   ```
   Get-ConfigZone
   ```

   b) Run the following commands for all the Citrix Cloud Connectors:

   ```
   Set-ConfigZone -Uid <Uid from above command output> -
       ExternalUid <RL ID noted at step 1>

   new-configedgeserver  <User friendly name> -MachineAddress "<
       Connector FQDN"> -Sid <Connector respective SID from step
       2> -uuid <Respective Edge server UUID from step 1> -ZoneUid
        <Uid from Get-ConfigZone output>
   ```

3. To use Rendezvous v1, enable Rendezvous within the Delivery Controller policies and ensure that the on-premises Delivery Controller is configured with the connector details to accept Rendezvous requests. For more information, see Rendezvous v1.
4. To use HDX adaptive transport with EDT, enable adaptive transport protocol within the Delivery Controller policies on your on-premises Delivery Controller. For more information, see HDX Adaptive transport with EDT support for Citrix Gateway service.

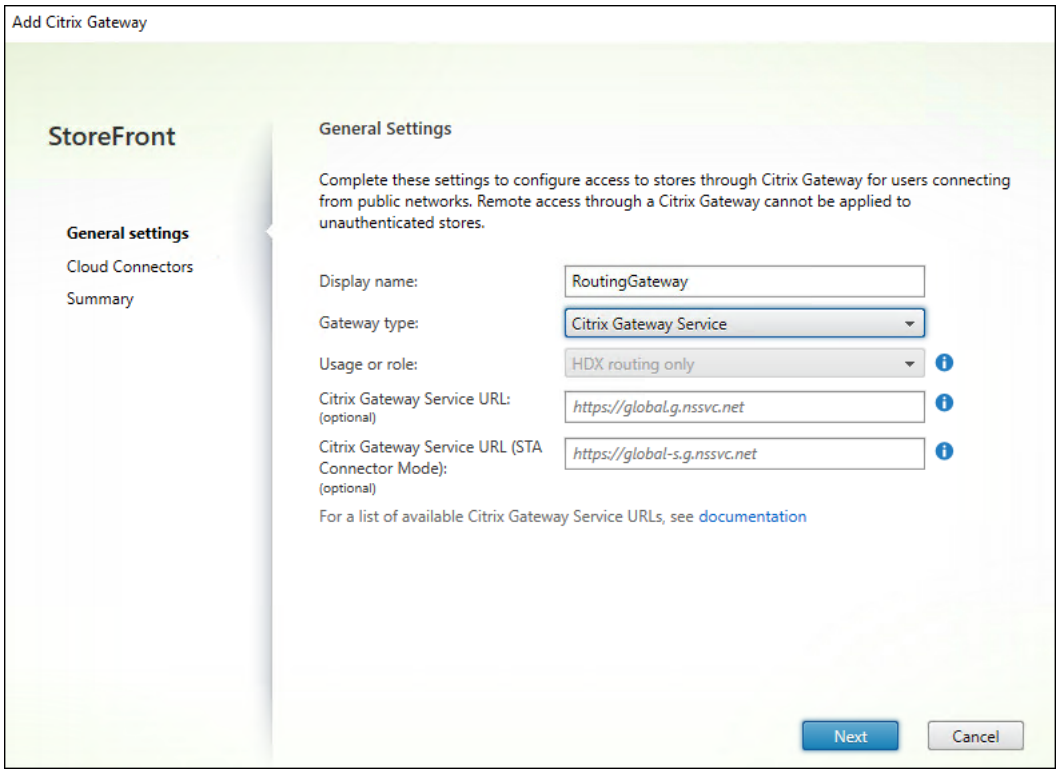
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure StoreFront to use Citrix Gateway service for HDX routing

For remote access to StoreFront, you must continue to use your existing NetScaler gateway. You can also use your NetScaler gateway for remote access to some resources, e.g. those in the same data center as the NetScaler gateway. For more information on configuring a NetScaler gateway for authentication in StoreFront, see Configure Citrix Gateways.

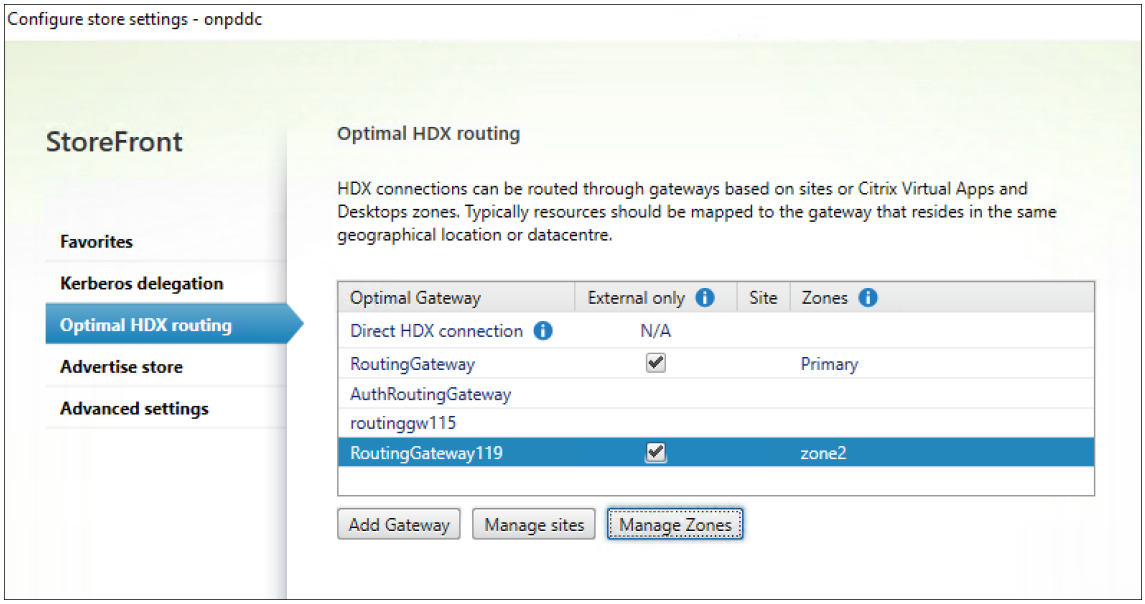
To configure Citrix Gateway service for HDX routing for some or all of your resources, create a gateway in StoreFront, and then use the Optimal Gateway Routing functionality of StoreFront to configure when it needs to be used:

1. Configure a gateway of type **Citrix Gateway Service** within StoreFront. Normally a single gateway is sufficient. However if you wish to use different geo-location rules for different sites or zones then you can configure multiple gateways with different gateway service URLs. For more information, see Add Citrix Gateway Service.



2. Choose for which sites or zones you wish HDX connections to be routed via those gateways. For more information, see Optimal HDX routing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



List of Points of Presence (PoPs) for Citrix Gateway service

September 9, 2026

> **Important:**
>
> The article CTX270584 is no longer maintained. Hence, refer to this page for the latest list of PoP FQDNs.

Citrix is adding more PoPs globally to ensure business continuity and quality service for Citrix Gateway service customers. The PoP lists are available in the following categories:

- PoPs for commercial regions
- PoPs for Google Cloud Platform (GCP) customers
- PoPs for Japan region
- PoPs for US Government region

The Citrix Workspace and Citrix Virtual Apps and Desktops customers might see network traffic potentially routed to new Citrix Gateway service FQDNs and destination addresses.

Firewall configuration

It is recommended to configure firewalls and Secure Web Gateways as mentioned in System and Connectivity Requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Customers might have hard-coded the FQDN or IP addresses to reach the Citrix Gateway service PoPs. They must update the firewall rules to allow the Citrix Gateway service-specific FQDN/IPs in the firewall and outbound proxies.

PoPs for commercial regions

September 9, 2026

For HDX™ traffic, we recommend the following configuration:

- `*.nssvc.net` (including all sub-domains)

If you have not enabled all the sub-domains, we recommend the following configurations (less preferred):

- `*.c.nssvc.net`
- `*.g.nssvc.net`

This wildcard applies to all existing and new PoP FQDNs. Customers who use wildcard-based allowlisting are not required to add the individual FQDNs.

> **Note:**
>
> - It is recommended to configure firewalls and Secure Web Gateways as mentioned in System and Connectivity Requirements.
> - If DNS forwarders are configured to allow recursive DNS resolution for specific domains, you must include `*.akadns.net` in the allowed list. This configuration enables the Citrix Cloud Connector, Citrix Virtual Apps and Desktops, or client to connect to the Citrix Gateway service.

Global FQDNs with defined set of PoPs

Type	FQDN	Purpose
Global	• global.g.nssvc.net • global-all.g.nssvc.net	Global FQDN

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Type	FQDN	Purpose
Global	• global-s.g.nssvc.net	Global FQDN including service continuity feature
Global	reg.c.nssvc.net	Connectors/VDA to register to Citrix Cloud
Azure only	azure-reg.c.nssvc.net	Connectors in Azure to register to Citrix Cloud

PoP FQDNs

The following table lists the Citrix Gateway service FQDNs associated with each Point of Presence (PoP):

Resource-side PoP FQDN (Cloud Connector or VDA): Used for connections to the Citrix Gateway service that originate from the resource side. Based on the configured connection path, the connection might originate from either a Citrix Cloud Connector or a Virtual Delivery Agent (VDA).

> **Important:**
>
> - Customers who already allow list `*.nssvc.net`, the more specific `*.g.nssvc.net` and `*.c.nssvc.net` domains, or the published Citrix Gateway service FQDNs, do not need to allow each PoP FQDN individually.
> - If your environment restricts Citrix Gateway service connectivity by IP address, review your current configuration against the published connectivity requirements.
> Citrix recommends using FQDN-based rules, because the destination IP addresses for the Citrix Gateway service can change.

PoP code	Resource-side PoP FQDN (Cloud Connector or VDA)	Cloud service provider	Country	Location
az-in-c	az-in-c-rdvz.g.nssvc.net	Azure	India	Pune
az-eu-c	az-eu-c-rdvz.g.nssvc.net	Azure	Germany	Frankfurt
az-us-c	az-us-c-rdvz.g.nssvc.net	Azure	USA	Iowa

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoP code	Resource-side PoP FQDN (Cloud Connector or VDA)	Cloud service provider	Country	Location
az-asia-hk	az-asia-hk-rdvz.g.nssvc.net	Azure	Hong Kong	Hong Kong
az-asia-se	az-asia-se-rdvz.g.nssvc.net	Azure	Singapore	Singapore
az-aus-e	az-aus-e-rdvz.g.nssvc.net	Azure	Australia	New South Wales
az-bz-s	az-bz-s-rdvz.g.nssvc.net	Azure	Brazil	Sao Paulo
az-ca-c	az-ca-c-rdvz.g.nssvc.net	Azure	Canada	Toronto
az-eu-n	az-eu-n-rdvz.g.nssvc.net	Azure	Ireland	Dublin
az-eu-w	az-eu-w-rdvz.g.nssvc.net	Azure	Netherlands	Amsterdam
az-in-s	az-in-s-rdvz.g.nssvc.net	Azure	India	Chennai
az-jp-e	az-jp-e-rdvz.g.nssvc.net	Azure	Japan	Tokyo
az-nw-e	az-nw-e-rdvz.g.nssvc.net	Azure	Norway	Oslo
az-uae-n	az-uae-n-rdvz.g.nssvc.net	Azure	UAE	Dubai
az-us-e	az-us-e-rdvz.g.nssvc.net	Azure	USA	Virginia
az-us-e2	az-us-e2-rdvz.g.nssvc.net	Azure	USA	Virginia
az-us-sc	az-us-sc-rdvz.g.nssvc.net	Azure	USA	Texas
az-us-w	az-us-w-rdvz.g.nssvc.net	Azure	USA	California
az-za-n	az-za-n-rdvz.g.nssvc.net	Azure	South Africa	Johannesburg
aws-eu-s	aws-eu-s-rdvz.g.nssvc.net	AWS	Italy	Milan

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoP code	Resource-side PoP FQDN (Cloud Connector or VDA)	Cloud service provider	Country	Location
aws-aus-e	aws-aus-e-rdvz.g.nssvc.net	AWS	Australia	Sydney
aws-asia-se	aws-asia-se-rdvz.g.nssvc.net	AWS	Singapore	Singapore
aws-asia-tw	aws-asia-tw-rdvz.g.nssvc.net	AWS	Taiwan	Taipei
aws-bz-s	aws-bz-s-rdvz.g.nssvc.net	AWS	Brazil	Sao Paulo
aws-ca-e	aws-ca-e-rdvz.g.nssvc.net	AWS	Canada	Montreal
aws-eu-c	aws-eu-c-rdvz.g.nssvc.net	AWS	Germany	Frankfurt
aws-eu-w	aws-eu-w-rdvz.g.nssvc.net	AWS	France	Paris
aws-in-sc	aws-in-sc-rdvz.g.nssvc.net	AWS	India	Hyderabad
aws-in-w	aws-in-w-rdvz.g.nssvc.net	AWS	India	Mumbai
aws-jp-w	aws-jp-w-rdvz.g.nssvc.net	AWS	Japan	Osaka
aws-uk-se	aws-uk-se-rdvz.g.nssvc.net	AWS	UK	London
aws-us-e	aws-us-e-rdvz.g.nssvc.net	AWS	USA	North Virginia
aws-us-nc	aws-us-nc-rdvz.g.nssvc.net	AWS	USA	Ohio
aws-us-w	aws-us-w-rdvz.g.nssvc.net	AWS	USA	North California

Regional FQDNs for geo-location routing

> **Notes:**
>
> Each geo-location has two FQDNS:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The FQDN ending with `rgn.g.nssvc.net` is the general FQDN.
- The FQDN ending with `rgn-s.g.nssvc.net` is the FQDN that includes the service continuity feature.
- Geo-location routing FQDNs do not require additional allow list entries during enhanced upgrades, as they automatically resolve to the active PoP infrastructure.

Geo-location	FQDNs	PoPs included
United States - East	• us-e-rgn.g.nssvc.net • us-e-rgn-s.g.nssvc.net	az-us-e, aws-us-e, aws-us-nc, az-us-e2
United States - Central and West	• us-wc-rgn.g.nssvc.net • us-wc-rgn-s.g.nssvc.net	az-us-w, aws-us-w, az-us-sc
United States	• us-rgn.g.nssvc.net • us-rgn-s.g.nssvc.net	az-us-sc, az-us-e, az-us-w, az-us-e2, aws-us-e, aws-us-w, aws-us-nc
United States - Azure only	• us-azure-rgn.g.nssvc.net • us-azure-rgn-s.g.nssvc.net	az-us-e, az-us-w, az-us-sc, az-us-e2
Europe	• eu-rgn.g.nssvc.net • eu-rgn-s.g.nssvc.net	aws-eu-c, aws-eu-w, az-eu-w, az-eu-n
Australia	• aus-rgn.g.nssvc.net • aus-rgn-s.g.nssvc.net	az-aus-e, aws-aus-e
Global - Azure only	• global-azure-rgn.g.nssvc.net • global-azure-rgn-s.g.nssvc.net	az-us-e, az-us-w, az-us-sc, az-bz-s, az-eu-w, az-eu-n, az-aus-e, az-asia-se, az-jp-e, az-uae-n, aws-in-w, az-in-s, az-in-s, az-uae-n, az-za-n, az-asia-se, az-jp-e, aws-in-sc, az-asia-hk, az-ca-c, az-us-e2, aws-asia-tw, aws-asia-se, az-nw-e aws-jp-w, aws-in-sc, az-in-s
Asia	• asia-rgn.g.nssvc.net • asia-rgn-s.g.nssvc.net	
India	• india-rgn.g.nssvc.net • india-rgn-s.g.nssvc.net	
Global - Alternate	• global-alt-rgn.g.nssvc.net • global-alt-rgn-s.g.nssvc.net	az-asia-se, az-aus-e, az-bz-s, az-ca-c, az-eu-n, az-eu-w, az-in-s, az-jp-e, az-nw-e, az-uae-n, az-us-e, az-us-sc, az-us-w, az-za-n, aws-aus-e, aws-bz-s, aws-ca-e, aws-eu-c, aws-in-w, aws-uk-se, aws-us-e, aws-us-nc, aws-us-w, az-us-e2, aws-asia-se, aws-eu-w, aws-in-sc, aws-jp-w

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoPs for Google Cloud Platform (GCP) customers

September 6, 2025

Citrix DaaS™ customers who have purchased subscriptions from the Google Cloud marketplace and are running their workloads on Google Cloud can use GCP PoPs.

> **Note:**
>
> It is recommended to configure firewalls and Secure Web Gateways as mentioned in System and Connectivity Requirements.

Support for PoPs in commercial regions

Support for PoPs in commercial regions for GCP customers is planned in the upcoming service release. With this support you can use the PoPs in commercial regions located across 5 continents. This support offers the following benefits:

- **Improved global access:** Reduced latency and improved performance for the GCP users worldwide.
- **Greater flexibility:** Choose the PoPs that best fit your needs and enhance cloud resiliency.

To use the PoPs in commercial regions, configure the firewall rules in VDA, Citrix Cloud Connector™, and Citrix Workspace™ app (client) according to the following instructions:

- Configure the firewall to establish connectivity between your resources and Citrix Cloud. For more information, see System and Connectivity Requirements.
- Configure the firewall for Citrix Cloud Connector. For more information, see Citrix Cloud Connector proxy and firewall configuration.
- Enable access to commercial region PoP FQDNs in Azure and AWS.

Global FQDNs with defined set of PoPs

Type	FQDN	Purpose
GCP only	gcp.g.nssvc.net	Global FQDN with GCP and commercial region PoPs
Global	reg.c.nssvc.net	Connectors/VDA to register to Citrix Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoP FQDNs

PoP code	PoP FQDN	Cloud service provider	Country	Location
gcp-us-sc	gcp-us-sc-rdvz.g.nssvc.net	GCP	USA	South Carolina
gcp-sz-zu	gcp-sz-zu-rdvz.g.nssvc.net	GCP	Switzerland	Zurich
gcp-us-la	gcp-us-la-rdvz.g.nssvc.net	GCP	USA	Los Angeles
gcp-uk-ln	gcp-uk-ln-rdvz.g.nssvc.net	GCP	UK	London
gcp-us-or	gcp-us-or-rdvz.g.nssvc.net	GCP	USA	The Dalles, Oregon
az-asia-hk	az-asia-hk-rdvz.g.nssvc.net	Azure	Hong Kong	Hong Kong
az-asia-se	az-asia-se-rdvz.g.nssvc.net	Azure	Singapore	Singapore
az-aus-e	az-aus-e-rdvz.g.nssvc.net	Azure	Australia	New South Wales
az-bz-s	az-bz-s-rdvz.g.nssvc.net	Azure	Brazil	Sao Paulo
az-ca-c	az-ca-c-rdvz.g.nssvc.net	Azure	Canada	Toronto
az-eu-n	az-eu-n-rdvz.g.nssvc.net	Azure	Ireland	Dublin
az-eu-w	az-eu-w-rdvz.g.nssvc.net	Azure	Netherlands	Amsterdam
az-in-s	az-in-s-rdvz.g.nssvc.net	Azure	India	Chennai
az-jp-e	az-jp-e-rdvz.g.nssvc.net	Azure	Japan	Tokyo
az-nw-e	az-nw-e-rdvz.g.nssvc.net	Azure	Norway	Oslo
az-uae-n	az-uae-n-rdvz.g.nssvc.net	Azure	UAE	Dubai
az-us-e	az-us-e-rdvz.g.nssvc.net	Azure	USA	Virginia

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoP code	PoP FQDN	Cloud service provider	Country	Location
az-us-sc	az-us-sc-rdvz.g.nssvc.net	Azure	USA	Texas
az-us-w	az-us-w-rdvz.g.nssvc.net	Azure	USA	California
az-za-n	az-za-n-rdvz.g.nssvc.net	Azure	South Africa	Johannesburg
aws-aus-e	aws-aus-e-rdvz.g.nssvc.net	AWS	Australia	Sydney
aws-bz-s	aws-bz-s-rdvz.g.nssvc.net	AWS	Brazil	Sao Paulo
aws-ca-e	aws-ca-e-rdvz.g.nssvc.net	AWS	Canada	Montreal
aws-eu-c	aws-eu-c-rdvz.g.nssvc.net	AWS	Germany	Frankfurt
aws-in-w	aws-in-w-rdvz.g.nssvc.net	AWS	India	Mumbai
aws-uk-se	aws-uk-se-rdvz.g.nssvc.net	AWS	UK	London
aws-us-e	aws-us-e-rdvz.g.nssvc.net	AWS	USA	North Virginia
aws-us-nc	aws-us-nc-rdvz.g.nssvc.net	AWS	USA	Ohio
aws-us-w	aws-us-w-rdvz.g.nssvc.net	AWS	USA	North California

PoPs for Japan region

September 9, 2026

For Japan customers, we recommend the following configuration:

- `*.*.nssvc.jp` (including all sub-domains)

If you have not enabled all the sub-domains, we recommend the following configurations (less preferred):

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `*.g.nssvc.jp`
- `*.c.nssvc.jp`

> **Note:**
>
> - Using the recommended addresses ensures continued operation of Citrix Gateway service as Citrix adds and retires addresses to enhance performance and availability.
> - We recommend you to configure firewalls and Secure Web Gateways according to Service connectivity requirements.
> - If DNS forwarders are configured to allow recursive DNS resolution for specific domains, you must include `*.akadns.net` in the allowed list. This configuration enables the Citrix Cloud Connector, client, or VDA to connect to the Citrix Gateway service. Complete this configuration before July 15, 2025 to ensure continued operation of the Citrix Gateway service.

Global FQDNs with defined set of PoPs

Type	FQDN	Purpose
Global	• global.g.nssvc.jp	Global FQDN
	• global-s.g.nssvc.jp	Global FQDN including service continuity feature
Global	reg.c.nssvc.jp	Connectors/VDA to register to Citrix Cloud

PoP FQDNs

PoP code	PoP FQDN	Cloud service provider	Country	Location
azjpc-jp-w	azjpc-jp-w-rdvz.g.nssvc.jp	Azure	Japan	Osaka
awsjpc-jp-e	awsjpc-jp-e-rdvz.g.nssvc.jp	AWS	Japan	Tokyo

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoPs for US Government region

September 9, 2026

For the US Government region, we recommend the following configuration:

- `*.*.nssvc.us` (including all sub-domains)

If you have not enabled all the sub-domains, we recommend the following configurations (less preferred):

- `*.g.nssvc.us`
- `*.c.nssvc.us`

> **Note:**
>
> - Using the recommended addresses ensures continued operation of Citrix Gateway service as Citrix adds and retires addresses to enhance performance and availability.
> - It is recommended to configure firewalls and Secure Web Gateways as mentioned in Connectivity requirements for Citrix Cloud Government.
> - To ensure that the Citrix Cloud Connector, client, or VDA resolve the necessary DNS queries to connect to the Citrix Gateway service, you must include `*.usgovtrafficmanager.net` in the allowed list of domains for recursive DNS resolution on your DNS forwarders. This configuration must be completed before April 27, 2025 to ensure continued operation of Citrix Gateway service.

Global FQDNs with defined set of PoPs

Type	FQDN	Purpose
Global	global.g.nssvc.us	Global FQDN for application launches
Global	reg.c.nssvc.us	Connectors/VDA to register to Citrix Cloud

PoP FQDNs

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PoP code	PoP FQDN	Cloud service provider	Country	Location
azusg-us-az	azusg-us-az-rdvz.g.nssvc.us	Azure	USA	US Gov Arizona
azusg-us-tx	azusg-us-tx-rdvz.g.nssvc.us	Azure	USA	US Gov Texas
azusg-us-va	azusg-us-va-rdvz.g.nssvc.us	Azure	USA	US Gov Virginia

Cloud Connector sizing and scale considerations for HDX proxy

September 9, 2026

Proper sizing and configuration of Citrix Cloud Connectors™ are crucial for high availability, stability, and efficient performance in HDX™ proxy deployments that do not use the Rendezvous v1 or v2 protocol (non-Rendezvous mode). Cloud Connectors serve as a vital proxy between the Citrix Gateway service and VDAs, making their optimization essential for seamless operations.

Tested maximum capacities and recommended machine configurations given in this article provide guidelines to ensure optimal performance and stability in HDX proxy deployments.

> **Note:**
>
> The recommendations apply to Cloud Connector deployments functioning as proxies for HDX proxy deployments in non-Rendezvous mode.

Improperly sized or misconfigured Cloud Connectors can result in performance bottlenecks, service disruptions, and instability. These challenges become more significant when handling large volumes of HDX proxy traffic between the Citrix Gateway service and VDAs. Proper sizing is essential to avoid these challenges and maintain a reliable user experience.

Recommendations

The following are the recommendations to determine the connector sizing:

- **Minimum Cloud Connectors:** 3 Cloud Connectors to ensure high availability.
- **Processors:** Intel Ice Lake, Cascade Lake, and newer processors.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Network:** Azure Accelerated Networking or equivalent network settings in other cloud environments or hypervisors.

Ensure you test in your specific environment to confirm the appropriate connector sizing.

Test conditions

- CPU and memory requirements are for the base Operating System (OS) and Citrix services only. Third-party applications and services might require more resources.
- Sessions are launched at a sustained rate.
- Tests are performed on a single Windows connector. A minimum of three connectors is recommended to ensure high availability.
- Tests are performed with the Cloud Connector configured with Intel Ice Lake or Cascade Lake processors.
- The client, Citrix Gateway service PoP, Cloud Connector, and VDAs are hosted on Azure in the same region. They establish end-to-end HDX sessions in non-Rendezvous mode. The sessions run through the test Cloud Connector while continuously simulating data packets.
- Tests are performed with the D2ds_v5, D4ds_v5, D8s_v5, and D16s_v4 virtual machines.

Test methodology

Tests are performed to apply load and evaluate the performance of the connector component. During testing, performance data such as CPU usage on the Cloud Connector and end-to-end latency are collected. Citrix proprietary simulation tools are used to simulate VDAs and sessions. These tools replicate the behavior of traditional VDAs and sessions while requiring fewer resources than hosting actual sessions and VDAs.

Recommendations for Cloud Connector sizing in this article are based on data gathered from the following tests:

- Tests performed to determine the number of connections and throughput supported without exceeding the following predefined conditions:
  - CPU usage of the Citrix Gateway service connector process < 70%
  - End-to-end latency < 50 ms
- Tests performed with minimum, average, and maximum packet sizes, using average values for results.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Summary of test findings

The following table lists the minimum recommended Cloud Connector CPU and other important configurations:

CPU	Memory (GB)	Number of concurrent HDX connections	HDX throughput (Mbps)
2	8	500	100
4	16	1000	200
8	32	2000	400
16	64	4000	700

> **Note:**
>
> The preceding concurrent HDX sessions and throughputs are recommendations and not hard limits. We recommend you to test your own HDX session limits in your specific environment.

FAQ

September 30, 2026

This section provides the FAQs on migrating Citrix ADC VPX to Citrix Gateway service for HDX proxy.

Can I use my on-premises configurations to port into Citrix Cloud™?

No, the underlying infrastructure and mechanisms are different. See section on enabling Citrix Gateway service.

Can I upload my portal customizations to Citrix Cloud?

This feature is not supported. However, there are few customization options with Citrix Cloud. Refer to the following link: Storefront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

I have enabled multi-factor or two factor authentication on-premises using VPX. Can I enable this on the cloud too?

The VPX provided with Citrix DaaS must be used for HDX proxy only (based on EULA) and not for authentication. Authentication on cloud is performed using either on-premises AD through a cloud connector or Azure Active Directory.

Can I use SmartControl, SmartAccess using cloud services?

The SmartControl feature is not supported in the Citrix Gateway service. The SmartAccess feature can be enabled using the Device Posture service (DPS) or Network location service (NLS) along with Adaptive Authentication or Conditional Authentication.

How can I do a phased migration to the Citrix Gateway service?

There is no configuration to support hybrid deployment (on-premises Citrix ADC VPX and Citrix Gateway service). It is recommended to perform a phased migration by enabling the Citrix Gateway service with a trial account (valid for a limited period) and testing it with a small group of users or preview users.

What is the minimum license required for the Citrix Gateway service?

Any customer using Citrix DaaS or Citrix Workspace is entitled to use Citrix Gateway service for HDX Proxy.

What is the bandwidth quota for customers with Citrix Universal™ Hybrid Multi-Cloud (UHMC) and Citrix Platform License (CPL)?

UHMC and CPL customers are entitled to the following bandwidth quota:

- User licensing: 2.5 GB per user per month
- Concurrent user licensing: 2.5 GB per user per month

UHMC and CPL are the new Stock Keeping Units (SKU). Other legacy SKUs (Citrix Universal subscriptions) are no longer available for renewals or contract extensions.

What happens after the bandwidth quota is exhausted?

When the bandwidth quota is exceeded, Citrix Gateway service continues to operate without any abrupt interruptions. There are no automated alerts for overusage but customers can monitor their

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Gateway service bandwidth usage in the Citrix Cloud portal under **Licensing Usage Insights -> Gateway Usage**.

Customers cannot purchase extra bandwidth, as Citrix® has discontinued the bandwidth-only SKU. Excessive bandwidth usage beyond the quota is reviewed during contract renewals.

What is the bandwidth quota for customers with a Citrix Universal subscription?

The bandwidth quota for customers with Citrix Universal subscription is as follows:

Citrix Gateway service + Citrix Workspace + Citrix DaaS packages:

Universal subscription edition	User licensing	Concurrent user licensing
DaaS Advance and Advance Plus editions	1 GB per user per month	2 GB per user per month
DaaS Premium and Premium Plus editions	5 GB per user per month	10 GB per user per month

Citrix Gateway service + Citrix Workspace packages:

Duration	User licensing	Concurrent user licensing
Term	1 GB per user per month	2 GB per user per month
	5 GB per user per month	10 GB per user per month
Annual	1 GB per user per month	2 GB per user per month
	5 GB per user per month	10 GB per user per month
Monthly	1 GB per user per month	2 GB per user per month
	5 GB per user per month	10 GB per user per month

The Citrix Universal subscription is no longer available for renewals or contract extensions and the customers are moved to UHMC and CPL subscription during renewal.

Where can I view the metrics of connections established through Citrix Gateway service?

The Connector statistics dashboard of the Citrix Analytics for Performance UI provides a comprehensive view of the resource consumption on the selected connector during the last 24 hours and a view of the synthetic latency calculated from the connector to the Citrix Gateway service PoPs in your virtual apps and desktops environment. For more information, see Connector Statistics.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.